Configuring IPX Services

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114051 Rev. A
August 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Configuring IPX Services

About This Guide

Audience xviii
Before You Begin xviii
Conventions xviii
Acronyms xix
Ordering Bay Networks Publications xxi

Technical Support and Online Services

Bay Networks Customer Service xxiv
Bay Networks Information Services xxv
World Wide Web xxv
Customer Service FTP xxv
Support Source CD xxvi
CompuServe xxvi
InfoFACTS xxvii
How to Get Help xxvii

Chapter 1
Starting IPX Services

Starting IPX 1-1
Deleting IPX from the Router 1-5

Chapter 2
IPX Concepts

Compatibility with Previous Versions of Bay Networks Software 2-1
About the IPX Protocol 2-2
Network-Level Services 2-3
Supported LAN Circuits, WAN Circuits, and Frame Formats 2-3
Types of IPX Configurations 2-5

For More Information about IPX 2-5

Chapter 3
Customizing IPX for LAN Media

Assigning a Unique Network Number 3-2
Enabling RIP and SAP on an Interface 3-2
Choosing a Frame Encapsulation Type 3-2
Specifying Multiple Interfaces per Circuit 3-3
Identifying a Circuit 3-5
Setting Additional Router Parameters 3-5
Configuring a Multiple-Host Router 3-5
Configuring a Single-Host Router 3-6
IPX Host ID Numbers 3-6
Setting a Host ID Number for IPX on a Token Ring Circuit 3-8
Token Ring MAC Address Selection 3-9
Customizing IPX 3-9

Chapter 4
Customizing IPX for WAN Media

IPX over WAN Media 4-1
Using IPXCP and IPXWAN 4-2
Running IPXWAN over PPP 4-2
Running IPXWAN over Frame Relay Permanent Virtual Circuits 4-3
Negotiating an IPXWAN Connection 4-3
Configuring an IPX Service to Run over a WAN 4-3
Assigning a Unique Network Number 4-4
Enabling RIP and SAP on an Interface 4-4
Identifying a Circuit 4-5
Entering an IPX Host ID Number for IPX over ATM 4-5
Enabling IPXWAN for an Interface 4-7
Assigning a Primary Network Number 4-7
Assigning a Common Network Number 4-7
Entering a Router Name 4-8
Indicating the Protocol Negotiated for an Interface 4-8
Sample IPXCP and IPXWAN Configurations 4-9
IPXCP Link Negotiation 4-9

IPXWAN Link Negotiation 4-10
IPXWAN and IPXCP Link Configurations 4-10
Configuration 1 (IPXWAN with IPXCP on Both Interfaces) 4-11
Configuration Guidelines -- Configuration 1 4-11
Configuration 2 (IPXWAN on Both Interfaces) 4-12
Configuration Guidelines -- Configuration 2 4-12
Configuration 3 (Only IPXCP on Both Interfaces) 4-12
Configuration Guidelines -- Configuration 3 4-12
Configuration 4 4-13
Customizing IPX 4-13

Chapter 5
Customizing IPX

Customizing Advanced Global Parameters 5-2
Setting the Maximum Number of Paths 5-2
Selecting a Log Filtering Mode 5-2
Specifying the Number of Maximum Path Splits 5-2
Specifying the Maximum Number of Destinations 5-3
Entering the Maximum Number of Services 5-3
Specifying the Granularity for Aging RIP and SAP Information 5-3
Specifying the Aging Pending Frequency 5-3
Enabling IPX Default Routing 5-4
Multipath Routing and Load sharing 5-4
Multipath Routing 5-4
Load Redistribution and Rerouting 5-6
Multipath Route Precedence/Priority 5-6
Multipath Configurations 5-7
Multiline Circuits 5-7
Selecting the GNS Response Mode 5-8
Customizing Interface Parameters 5-9
Enabling IPX Routing on an Interface 5-9
Entering a Symbolic Name for an Interface 5-9
Assigning a Host Number to an Interface 5-9
Enabling Source Routing for an Interface on a Token Ring Circuit 5-10
Entering a Broadcast Address 5-10
Entering a Multicast Address 5-10

Responding to IPX Watchdog Packets 5-11
Setting Delay Time 5-11
Specifying Throughput 5-11
Setting Stabilization Timer Delay 5-12
Handling Packets Associated with Upper-Layer Protocols 5-12
The Routing Information Protocol (RIP) 5-13
Enabling RIP on the Router 5-14
Choosing the Routing Method 5-14
Setting a Cost for an Interface 5-15
Specifying the Maximum Number of Hops 5-16
Indicating the Number of Next-Hop Hosts 5-17
Enabling RIP Listen and Supply Functions 5-17
Determining the Pace of RIP Packets 5-17
Configurable RIP Timers 5-18
Adjusting the RIP Packet Size 5-19
Enabling Multicast Transmission of RIP Packets 5-20
Configurable Split Horizon 5-20
Fully Meshed Networks 5-20
Nonfully Meshed Networks 5-21
Updating Routers About a Failed Route 5-23
Advertising Default Routes in RIP Packets 5-23
Accepting Default Route Information 5-23
Customizing SAP Parameters 5-23
NetWare Directory Services (NDS) and SAP 5-24
SAP and the NetWare Bindery (NetWare 3.*x* and Earlier) 5-24
Configurable SAP Timers 5-25
SAP via Default Route 5-26
Enabling SAP Listen and Supply Functions 5-26
Determining the Pace of SAP Packets 5-26
Adjusting the SAP Packet Size 5-27
Responding to Nearest Server Requests 5-27
Using a Multicast Address 5-27
Saving the Service Name 5-27
Transmitting and Receiving SAP Updates Over the Same Interface 5-28
Updating Routers About a Failed Service 5-28

Using Static Services 5-28
Enabling Static Services 5-31
Specifying the Network Address of a Service 5-32
Specifying the Address of the Host that Provides a Service 5-32
Assigning a Symbolic Name to Your Service 5-32
Entering the Service Type Number 5-32
Entering the Socket Address of a Service 5-33
Entering the Hop Count 5-33
Customizing NetBIOS Static Routing 5-33
Activating the Static Route Record in the NetBIOS Routing Table 5-35
Entering the Name of the NetBIOS Target Server 5-35
Entering the Target Network Address 5-35
Directing a NetBIOS Packet Using Nonstandard Static Routing 5-36
Directing a NetBIOS Packet Using Standard Static Routing 5-37
NetBIOS Broadcast Filters 5-37
Configuring an Adjacent Host for an Interface 5-40
Making the Adjacent Host Record Active 5-40
Entering the ID of the Adjacent Host 5-41
Entering a WAN Address or a DLCI 5-41
Dial Services 5-41
Using Dial-on-Demand Service 5-42
Using Static Routing with Dial-on-Demand 5-43
Tips for Using Dial-on-Demand with IPX 5-44
Local IPX Watchdog Acknowledgment 5-44
Local SPX Keep-Alive Acknowledgment 5-45
Dial Optimized Routing 5-46
Default IPX Dial Optimized Routing Filters 5-46
Configuring the Routing Update Delay Timer 5-47
RIP/SAP Triggered Updates 5-47
Determining the Frequency of Scheduled Updates 5-47
Configuring RIP and SAP Broadcast Timers 5-48
Using Static Routes 5-50
Specifying the Target Network Address 5-52
Entering the Next-Hop Host 5-52
Entering the Hop Count 5-52

Setting the Timer Ticks 5-53
Using Route Filters 5-53
Using SAP Filters 5-54
Using Wildcards and Pattern Matching with SAP Filters 5-57
Using Wildcards with SAP Filters 5-57
Using Pattern Matching with SAP Filters 5-59
An Example of Using SAP Filters 5-63
Editing Service Name Filter Parameters 5-64
Enabling an IPX Service Name Filter 5-65
Entering the Target Service Name 5-65
Entering the Target Service Type 5-65
Setting the Filter Priority 5-65
Applying Filters to Inbound or Outbound Packets 5-66
Specifying the Protocol 5-66
Specifying How to Process SAP Advertisements 5-66
Specifying a Cost 5-67
Source Route Bridge Endstation Support 5-67
IPX Ping Support 5-69
Role of Bay Networks Routers in a Client/Server Connection 5-70
Example: Client/Server Connection via Bay Networks Router 5-71

Appendix A
IPX Parameters

IPX Configuration Parameters A-1
IPXWAN Configuration Parameters A-7
IPX Global Parameters A-9
IPX Advanced Global Parameters A-13
IPX Interface Parameters A-21
IPX Change Circuit Parameters A-29
IPX RIP Circuit Parameters A-34
IPX SAP Circuit Parameters A-40
IPX NetBIOS Static Route Configuration Parameters A-45
IPX NetBIOS Static Route Parameters A-47
Adjacent Hosts Configuration Parameters A-49
IPX Adjacent Hosts Parameters A-51
IPX Static Route Configuration Parameters A-53

IPX Static Route Parameter Descriptions A-56
IPX Static Service Configuration Parameters A-58
IPX Static Service Parameters A-61
Route Filter Configuration Parameters A-64
IPX Route Filter Parameters A-66
Service Network Filter Configuration Parameters A-71
IPX Service Network Filter Parameters A-74
IPX Service Name Filter Configuration Parameters A-79
IPX Service Name Filter Parameters A-81

Appendix B
IPX Default Parameter Settings

IPX Global Parameter Defaults B-1
IPX Advanced Global Parameter Default Values B-2
IPX Interface Parameter Default Values B-3
IPX Change Circuit Parameter Default Values B-4
IPX RIP Circuit Parameter Default Values B-4
IPX SAP Circuit Parameter Default Values B-5
IPX NetBIOS Static Route Configuration Parameter Default Values B-6
IPX NetBIOS Static Route Parameter Default Values B-6
Adjacent Host Configuration Parameter Default Values B-6
IPX Adjacent Hosts Parameter Default Values B-7
IPX Static Route Configuration Parameter Default Values B-7
IPX Static Route Parameter Default Values B-7
IPX Static Service Configuration Parameter Default Values B-8
IPX Static Services Parameter Default Values B-8
Route Filter Configuration Parameter Default Values B-9
IPX Route Filter Parameter Default Values B-9
SAP Network Filter Configuration Parameters B-10
IPX SAP Network-Level Filter Parameter Descriptions B-10
IPX Server-Level Filter Configuration Parameter Descriptions B-11
IPX SAP Server-Level Parameter Default Values B-12

Appendix C
Common Service Types and Identifiers

Appendix D
Sample IPX Configuration

Configuration Particulars D-2
Router 1 ..... D-2
Router 2 ..... D-3

Index

Figures

Figure 3-1. Multiple IPX Interfaces per Physical Circuit 3-4
Figure 3-2. Frames Received at a Logical Interface 3-7
Figure 3-3. Frames Issued from a Logical Interface 3-8
Figure 4-1. Frames Received at a Logical Interface 4-5
Figure 4-2. Frames Issued from a Logical Interface 4-6
Figure 4-3. IPXCP and IPXWAN Configurations 4-9
Figure 5-1. IPX Multipath 5-5
Figure 5-2. IPX Multipath Routing -- Equal Least-Cost Routes 5-6
Figure 5-3. IPX Configurable RIP Interface Cost 5-16
Figure 5-4. IPX Configurable RIP Timers 5-19
Figure 5-5. Split Horizon Enabled in a Fully Meshed Network 5-21
Figure 5-6. Split Horizon Disabled in a Nonfully Meshed Network 5-22
Figure 5-7. Static Service Network Configuration 5-30
Figure 5-8. IPX SAP Filters Prohibiting SAP Broadcasts 5-31
Figure 5-9. NetBIOS Static Routes 5-34
Figure 5-10. NetBIOS Packet Filtering 5-38
Figure 5-11. NetBIOS Packet Flow 5-39
Figure 5-12. NetBIOS Broadcast Filtering 5-40
Figure 5-13. Dial-on-Demand Service 5-43
Figure 5-14. IPX Static Routes 5-51
Figure 5-15. SAP Filtering 5-55
Figure 5-16. IPX Routers Source Routing Across a Token Ring Network 5-68
Figure 5-17. Sample IPX Network 5-72
Figure A-1. IPX Configuration window A-2
Figure A-2. IPXWAN Configuration Window A-7
Figure A-3. Edit IPX Global Parameters window. A-9
Figure A-4. IPX Advanced Global Parameters Window A-13
Figure A-5. IPX Interfaces Window A-21
Figure A-6. IPX Change Circuit Window A-29

Figure A-7. IPX RIP Circuit Window A-34
Figure A-8. IPX SAP Circuit Window A-40
Figure A-9. IPX NetBIOS Static Route Configuration Window A-45
Figure A-10. IPX NetBIOS Static Routes Window A-47
Figure A-11. IPX Adjacent Hosts Configuration Window A-49
Figure A-12. IPX Adjacent Hosts Window A-51
Figure A-13. IPX Static Route Configuration Window A-53
Figure A-14. IPX Static Routes Window A-56
Figure A-15. IPX Static Service Configuration Window A-58
Figure A-16. IPX Static Services Window A-61
Figure A-17. IPX Route Filter Configuration Window A-64
Figure A-18. IPX Route Filters Window A-66
Figure A-19. IPX Service Network Filter Configuration Window A-71
Figure A-20. IPX Service Network Filters Window A-74
Figure A-21. IPX Service Name Filter Configuration Window A-79
Figure A-22. IPX Service Name Filters Window A-81
Figure D-1. Sample IPX Configuration D-2

Tables

Table 2-1. LAN Circuit and Frame Support for IPX Interfaces 2-4
Table 2-2. WAN Circuit and Frame Support for IPX Interfaces 2-4
Table 4-1. Configuration Table for IPX Over WAN Media 4-11
Table 5-1. Characters in SAP Pattern Matching Filters 5-59
Table 5-2. Concatenation Rules and Operators 5-61
Table B-1. IPX Global Parameter Default Values B-1
Table B-2. IPX Advanced Global Parameter Default Values B-2
Table B-3. IPX Interface Parameter Default Values B-3
Table B-4. IPX Change Circuit Parameter Default Values B-4
Table B-5. IPX RIP Circuit Parameter Default Values B-4
Table B-6. IPX SAP Circuit Parameter Default Values B-5
Table B-7. NetBIOS Static Route Configuration Parameter Default Values B-6
Table B-8. IPX NetBIOS Static Route Parameter Default Values B-6
Table B-9. Adjacent Host Configuration Parameter Default Values B-6
Table B-10. IPX Adjacent Hosts Parameter Default Values B-7
Table B-11. IPX Static Route Configuration Parameter Default Values B-7
Table B-12. IPX Static Route Parameter Default Values B-7
Table B-13. IPX Static Service Configuration Parameter Default Values B-8
Table B-14. IPX Static Services Parameter Default Values B-8
Table B-15. Route Filter Configuration Parameter Default Values B-9
Table B-16. IPX Route Filter Parameter Default Values B-9
Table B-17. SAP Network Filter Configuration Parameter Default Values B-10
Table B-18. SAP Network-Level Filter Parameter Default Values B-10
Table B-19. IPX Server-Level Filter Configuration Parameter Default Values B-11
Table B-20. IPX SAP Server-Level Parameter Default Values B-12
Table C-1. Service Types and Identifiers C-1

About This Guide

If you are responsible for configuring and managing Bay Networks™ routers, read this guide to discover how to customize Bay Networks router software for Internet Packet Exchange (IPX) services.

Configuring IPX Services offers

- A quick start procedure for starting IPX services (refer to Chapter 1)
- An overview of the IPX protocol and a description of how Bay Networks routing services work (refer to Chapter 2)
- Instructions on enabling IPX and IPXWAN (refer to Chapters 3 and 4)
- Instructions on editing IPX global and interface parameters and configuring IPX services (refer to Chapter 5)
- A detailed description of each IPX parameter (refer to Appendix A)
- A list of the default settings for the IPX parameters (refer to Appendix B)
- A list of common service types and identifiers (refer to Appendix C)
- Sample IPX configurations (refer to Appendix D)

For information and instructions about the following tasks, see *Configuring Routers*:

- Retrieving a configuration file
- Rebooting the router with a configuration file

Audience

Written for system and network managers, this guide describes how to configure the Bay Networks implementation of IPX protocol to suit your environment.

Whether you use Novell software or a combination of Novell and compatible third-party systems, this guide provides the options you need to communicate and share resources on your network.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers*, *Connecting AN and ANH Systems to a Network*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–10.xx to Version 11.0*.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.

brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

AUI	Attachment Unit Interface
ARE	All route explore
ATM	Asynchronous transfer mode
BOOTP	Bootstrap Protocol
BRI	Basic Rate Interface
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
CSMA/CD	carrier sense multiple access with collision detection
DLCMI	Data Link Control Management Interface
GUI	graphical user interface

HDLC	high-level data link control
IP	Internet Protocol
IPX	Internet Packet Exchange Service
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union–Telecommunications (formerly CCITT)
LAN	local area network
MAC	media access control
MAU	media access unit
MDI-X	media-dependent interface with crossover
MIB	management information base
NBMA	nonbroadcast multi-access
NCP	Network Core Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First (Protocol)
PDN	Public Data Network
PPP	Point-to-Point Protocol
RIF	Routing information field
RIP	Routing Information Protocol
SAP	Service Advertisement Protocol
SMDS	switched multimegabit data service
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
SRE	specific route explore
STP	shielded twisted-pair
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TPE	twisted-pair Ethernet
UTP	unshielded twisted-pair
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Starting IPX Services

IPX is the network-layer routing protocol used in the NetWare environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network.

If you are already familiar with IPX and want to get the protocol up and running quickly, follow the steps below to start IPX using Bay Networks default settings. You supply only the necessary configuration settings and accept all other default settings.

For conceptual information on IPX, refer to Chapter 2. For information on customizing the way IPX runs on the router to meet your needs, refer to Chapters 3 through 5. For information on changing the default settings, refer to Appendix B.

Starting IPX

IPX can operate over LAN or WAN media. This section describes how to get IPX and, optionally, IPXWAN services up and running on a circuit. We assume that you have read *Configuring Routers*.

To use IPX, first start Site Manager and then follow these steps:

1. **Select Configuration Manager in either local, remote, or dynamic mode from the Tools menu.**

   The Configuration Manager window appears.

2. **Open a configuration file if local or remote mode is selected.**

3. **Select a circuit**

   Select the circuit you want to configure. If this is a local mode configuration, specify router hardware.

4. **Select a protocol.**

   If you are running IPX over a WAN, select a WAN protocol (usually PPP or Frame Relay).

Note: Selecting Frame Relay, PPP, or SMDS on a WAN circuit automatically enables protocol prioritization

---

5. **Select IPX or RIP/SAP (which automatically selects IPX as well) from the Select Protocols window.**

   If you selected RIP/SAP from the Select Protocols window, the router enables both RIP and SAP services using their default values. To change any of their default values, refer to Appendix B.

   The IPX Configuration window appears.

6. **Complete the IPX Configuration window.**

   If you are configuring a LAN or WAN circuit, you must supply the following information:

   - A *configured network number.*

     A configured network number is any valid IPX network address in hexadecimal notation.

     If you are configuring this interface as Unnumbered RIP, supply the value zero for the configured network number.

     If you are trying to establish a connection to a Series 5 Bay Networks router, or a router that does not implement IPXWAN or PPP, then you must enter a nonzero network address (for example, the network address of the link).

     If you are configuring an IPX interface that will enable IPXWAN services, do not supply a configured network number.

Site Manager: Configured Network Number (hex) parameter: page A-2

- The *encapsulation method.*

  By default, IPX supplies an encapsulation method that is media dependent. The encapsulation method supports communication on a specific logical link. Check to make sure that the supplied encapsulation method matches the one the clients and servers on the same logical network use, and is appropriate for the physical circuit, as follows:

  – Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.

  – Token ring circuits support LSAP and SNAP frames.

  – Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.

  – FDDI circuits support LSAP and SNAP frames.

  – HSSI circuits support PPP and SNAP frames.

  – ISDN circuits support PPP frames.

Site Manager: Configured Encaps parameter: page A-4

If you are configuring an IPXWAN circuit, you must also supply the following information:

- A *common network number.*

  The common network number is a network number that you assign to the WAN circuit. If this router is the master during the IPXWAN negotiation and RIP is selected as the routing protocol, then the common network number is used as the IPX network number for the circuit.

  There is no default for the common network number. You must supply an IPX common network number in hexadecimal format. Valid common network numbers range from 0x00000000 to 0xFFFFFFFD. Do not use the value 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.

Site Manager: Common Network Number (hex) parameter: page A-5

- A *negotiated protocol*.

  The negotiated protocol specifies the protocol that the router supports for the exchange of routing information over this WAN circuit. You can specify either RIP or Unnumbered RIP as the negotiated protocol. For a description of RIP, refer to Chapter 5.

Site Manager: Negotiated Protocol(s) parameter: page A-6

7. **Click on OK.**

   If you did not enable IPXWAN services, IPX is now completely configured using the information you supplied and all other supplied default values. You can now use IPX. If you want to change any of the supplied defaults to fine-tune the way IPX works, refer to Appendix A.

   If you enabled IPXWAN services in the IPX Configuration window, the IPXWAN Configuration window appears. You must supply the following information

   - A *router name*.

     The router name is any symbolic name that you choose for the router. You must choose a name that is unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork. Any IPXWAN (RFC1634-compliant) interface in the node uses this name to identify itself to the IPX router or server at the opposite end of the WAN data link.

Site Manager: Router Name parameter: page A-7

   - A *primary network number.*

     A primary network number is a unique string of up to 8 hexadecimal characters that specifies an IPX network number for IPXWAN link negotiation on all slots. You can enter any unused value between 0x00000001 and 0xFFFFFFFD.

     The value you enter for the primary network number determines whether the local or remote router on the WAN circuit serves as the IPX Link Master. The node with the highest primary network number becomes the IPX Link Master.

Site Manager: Primary Net Number (hex) parameter: page A-8

8. **Click on OK.**

Deleting IPX from the Router

You can use Site manager to delete IPX from the router.

1. **Select Configuration Manager in either local, remote or dynamic mode from the Tools menu.**

   The Configuration Manager window appears.

2. **Select Protocols > IPX > Delete IPX option from the menu bar.**

   A confirmation window appears.

3. **Click on OK.**

   IPX is no longer configured on the router and the Configuration Manager window reappears.

Note: If you delete IPX, the connectors for those interfaces on which IPX was the only protocol enabled are no longer highlighted in the Configuration Manager window. Interfaces must be reconfigured for these connectors; see *Configuring Routers* for instructions.

Chapter 2
IPX Concepts

This chapter describes some of the IPX concepts you will need to know before you begin configuring an interface on a circuit. It provides an overview of the IPX protocol, the network-level services provided by a Bay Networks router running IPX, the types of LAN and WAN circuits IPX supports, and some basic types of IPX configurations.

Compatibility with Previous Versions of Bay Networks Software

This guide describes only the Version 11.0 Bay Networks router software.

Site Manager 5.0 and Router Software Version 11.0 are backward compatible with earlier versions of the router code. You can boot an IPX configuration that operates with an earlier version (for example, 8.10) on a router that has Version 11.0 software, and the software will update the configuration. You can then go into dynamic mode (or save the updated configuration and go into remote mode) and edit any of the new parameters. When you save the edited configuration, you're saving a Version 11.0 file.

In local mode, Site Manager will run IPX configurations from an earlier version using the Management Information Base (MIB) for that version instead of the MIB for Version 11.0. If you choose to continue using a router configuration that you configured under a software version earlier than 11.0 without updating it, you will not get the Version 11.0 features, and you must use the Version 8.10 guide *Customizing IPX Services* instead of this guide.

About the IPX Protocol

The Internet Packet Exchange protocol is the Novell, Inc., adaptation of the Xerox Network System (XNS) protocol. IPX has the following characteristics:

- It is a *connectionless datagram* delivery protocol. *Connectionless* means that it does not need a channel established for packet delivery. A *datagram* is a unit of data that contains all the addressing information required for it to be delivered to its destination. The path or route that one datagram follows to reach a destination is independent of the path or route that another datagram may follow to reach the same destination.
- It does not guarantee the delivery of packets. Higher-level protocols assume the responsibility for reliability. The higher-level protocols that IPX uses are SPX and NCP.
- It uses the Internet Data Packet (IDP) format.

IPX is the network-layer routing protocol used in the NetWare environment. The primary tasks of IPX are addressing, routing, and switching information packets from one location to another on a network. The network interface card (NIC) in a client provides network node addressing. IPX defines the *internetwork* and *intranode* addressing as follows:

- Network numbers form the basis of the IPX *internetwork* addressing scheme for sending packets between network segments. Every network segment of an internetwork is assigned a unique network address by which routers forward packets to their final destination network. A network number in the NetWare environment consists of 8 hexadecimal characters. In the following example, *0x* indicates that this is a hexadecimal number, and *n* is any hexadecimal character.

  0xnnnnnnnn

Socket numbers are the basis for an IPX *intranode* address; that is, the address of individual entities within a node. They allow a process (for example, RIP or SAP) to distinguish itself to IPX. To be able to communicate on the network, the process must request a socket number. Any packets IPX receives addressed to that socket are then passed on to the process within the node.

Network-Level Services

A Bay Networks router running IPX provides the following network-level support:

- Dynamic routing of IPX packets
- Multiple IPX interfaces per circuit
- IPX over WAN media
- IPXWAN and IPXCP
- Routing Information Protocol (RIP and Unnumbered RIP)
- Service Advertising Protocol (SAP)
- Static Route support
- Default Route support
- Adjacent Host support
- Dial-on-Demand support

Dynamic routing occurs normally on any IPX interface; brief descriptions of the other supported capabilities follow.

Supported LAN Circuits, WAN Circuits, and Frame Formats

IPX supports various combinations of physical circuits and data-link layer frame formats. You can choose the ones that are appropriate for the types of clients and applications on your network.

Table 2-1 shows the types of LAN circuits and frame formats supported by Bay Networks routers running IPX.

Table 2-1. LAN Circuit and Frame Support for IPX Interfaces

Circuit Type	Frame Type -- Novell Terminology	Frame Type -- Bay Networks Terminology
Ethernet	ETHERNET_II ETHERNET_802.2 ETHERNET_802.3 ETHERNET_SNAP	ETHERNET LSAP NOVELL SNAP
TOKEN RING	TOKEN-RING TOKEN-RING_SNAP	LSAP SNAP
FDDI	N/A	LSAP SNAP

Table 2-2 shows the relationships between the types of WAN circuits, the WAN protocols, and the frame formats supported by Bay Networks routers running IPX.

Table 2-2. WAN Circuit and Frame Support for IPX Interfaces

Circuit Type	WAN Protocol	Frame Type -- Bay Networks Terminology
Synchronous: --V.35 --RS-232/V.24 --RS-422/423 --X.21 --T1/Fractional T1 --E1/Fractional E1	These protocols apply to all these circuit types: --ATM --Frame Relay --PPP --SMDS --X.25 Point-to-Point --X.25 PDN --Bay Networks Point-to-Point	 SNAP SNAP PPP SNAP ETHERNET RFC 1356 ETHERNET
HSSI	ATM Frame Relay PPP SMDS Bay Networks Point-to-Point	SNAP SNAP PPP SNAP ETHERNET
ISDN	PPP	PPP

You can use these tables when you select an encapsulation method on the IPX Configuration window. For more information about the encapsulation method, refer to “Configured Encaps” on page A-4.

Types of IPX Configurations

The basic types of IPX configurations are

- Standard, with two possible configurations:
  - -- *Multiple-Host Router.* This common configuration supports one IPX interface per circuit; each interface has a unique IPX host number.
  - -- *Single-Host Router.* This configuration supports one IPX interface per circuit; every interface shares the same global (“boxwide”) IPX host number.
- Special, also with two possible configurations:
  - -- *Multiple Interfaces per Circuit.* This special configuration supports as many IPX interfaces per circuit as there are frame encapsulation types for the given circuit type.
  - -- *Multiple Circuits per Segment.* This special configuration supports either concurrent bridging and IPX routing or IPX multiline.

For More Information about IPX

The following documents provide technical details about IPX protocol implementation.

RFC 1634: *Novell IPX over Various WAN Media (IPXWAN)*. (Obsoletes RFC 1551 and RFC 1362.)

RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*.

Novell, Inc. *Advanced NetWare, V.2.0 Internet Packet Exchange Protocol (IPX) with Asynchronous Event Scheduler.* March 19, 1986.

Novell, Inc., *IPX Router Specification.* October 1993.

Novell Press/Sybex, *Novell’s Guide to NetWare LAN Analysis*, Laura Chappell and Dan E. Hawkes. 1994.

Chapter 3
Customizing IPX for LAN Media

You can use IPX services over either a LAN or a WAN. This chapter discusses issues related specifically to using IPX over a LAN. For information specific to using IPX over a WAN, see Chapter 4. For information on how to customize IPX features for use on both a LAN and a WAN refer to Chapter 5.

When you configure an IPX service to run over a LAN, you need to make sure the following parameters have the appropriate settings in the IPX configuration.

- Configured Network Number (required)
- RIP/SAP
- Configured Encapsulation (required)
- Circuit Index

If you want to configure multiple IPX interfaces on a circuit, and a multiple-host router, set the following parameters in addition to the parameters you set on the IPX Configuration window.

- Enable parameter on the IPX Global Parameters window
- Multiple Host Address Enable on the IPX Global Parameters window
- Host Number on the IPX Interfaces window

Assigning a Unique Network Number

When you initially add an IPX interface to the router configuration, You must enter the network number of the IPX network segment associated with that interface. The network number must be unique among all other network numbers assigned throughout the IPX internetwork.

Site Manager: Configured Network Number (hex) parameter: page A-2

Enabling RIP and SAP on an Interface

The Configuration Manager sets the default for this parameter based on your selection in the Select Protocols window. If you selected RIP/SAP, both RIP and SAP are enabled. You can disable both RIP and SAP using the IPX Configuration window. You can also disable and re-enable just RIP or just SAP using the RIP Circuit window or the SAP Circuit window, which are available via the IPX Interfaces window.

Site Manager: RIP/SAP parameter: page A-3

Choosing a Frame Encapsulation Type

When you add an IPX interface to the router configuration, you must specify the type of frame encapsulation required for communication between all hosts on the same IPX logical network within the overall IPX internetwork.

Choose the encapsulation method that is appropriate for the type of physical circuit you are configuring.

- Ethernet circuits support Ethernet, LSAP (802.2), Novell (802.3), and SNAP frames.
- Token Ring circuits support LSAP and SNAP frames.
- FDDI circuits support LSAP and SNAP frames.

Site Manager: Configured Encaps parameter: page A-4

Specifying Multiple Interfaces per Circuit

You can configure one or more IPX interfaces per physical circuit. The number of IPX logical interfaces you can configure on a circuit equals the number of unique frame formats available for that circuit type. (Refer to Table 2-1 for details on circuit types and frame formats.)

For example, the Bay Networks router supports four unique frame formats that are suitable for communication over an Ethernet LAN segment. This means that you can configure four *different* encapsulations for four independent IPX interfaces on a single Ethernet circuit (Ethernet, Novell, LSAP, and SNAP). Each interface and encapsulation configured on a circuit supports a different logical network. To differentiate between IPX interfaces configured on the same physical circuit, the Bay Networks router uses the unique network address and frame format that you assign to each interface.

By supporting multiple IPX interfaces on a single physical circuit, a Bay Networks router can service clients on independent *logical* LANs that coexist on the same *physical* LAN segment.

In Figure 3-1, each client on the right side of the router has a different logical network address and uses a different encapsulation method. If all clients need to access Server 1, then only Interface 2 of the router needs to support all the different encapsulation methods and multiple logical network addresses for the workstations. Interface 1 of the router needs to support only the SNAP encapsulation method that Server 1 supports.

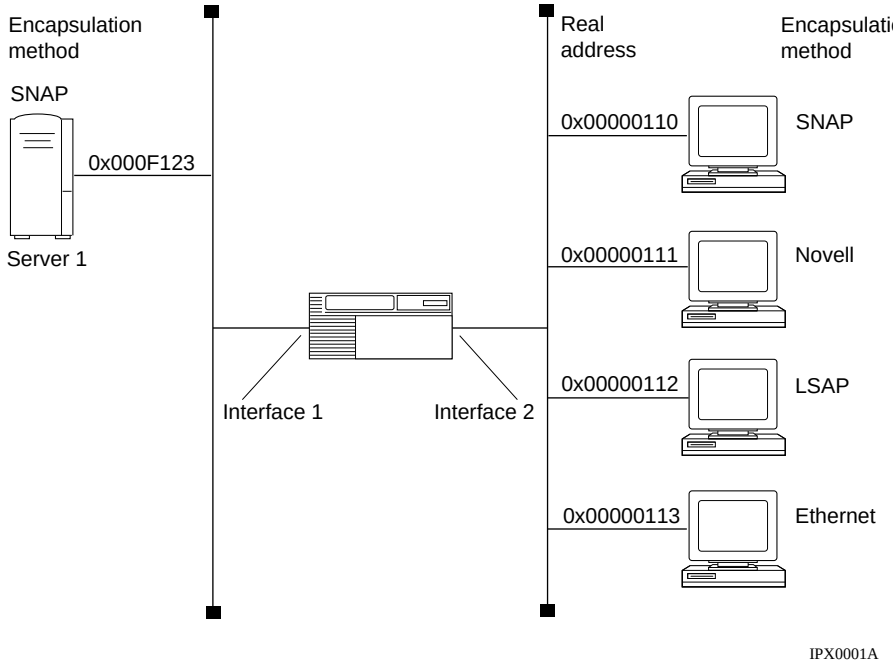

Figure 3-1. Multiple IPX Interfaces per Physical Circuit

Note: NetWare users -- If you are upgrading client and server stations on your network to Novell NetWare Version 4.*x*, you can use the multiple-interface-per-circuit capability to gradually migrate stations on the same network segment to NetWare Version 4.*x* (that is, from one logical network to another, independent logical network).

For example, you can upgrade and migrate NetWare clients from a logical network that supports only Novell (802.3) encapsulated frames to a logical network that supports a more versatile LSAP (802.2 frame type).

You use the Site Manager software to choose the following encapsulation methods that are appropriate for the type of physical circuit you are configuring.

- Ethernet circuits support Ethernet, LSAP (802.2), Novell (802.3), and SNAP frames.
- Token Ring circuits support LSAP and SNAP frames.
- FDDI circuits support LSAP and SNAP frames.

Site Manager: Enable parameter: page A-10
Site Manager: Configured Encaps parameter: page A-4

For more information about configuring a physical LAN circuit, refer to *Configuring Routers*.

Identifying a Circuit

The Site Manager automatically assigns a circuit identifier to each circuit that you create on an IPX router. You can assign a specific circuit identifier, if necessary.

Site Manager: Circuit Index parameter: page A-4

Setting Additional Router Parameters

You can configure your Bay Networks router to serve as either a multiple-host or single-host router.

Configuring a Multiple-Host Router

A multiple-host router is a common configuration that supports one IPX interface per circuit, and each interface has a unique IPX host number. For this configuration, leave the Multiple Host Address Enable parameter at its default setting, Enable. The host number of each IPX interface is based on the MAC address of the underlying circuit. For Ethernet or FDDI circuits, you can specify the multiple host address in the Host Number field on the IPX Interface window.

Site Manager: Multiple Host Address Enable parameter: page A-10

Configuring a Single-Host Router

For this configuration, you need to set the Multiple Host Address parameter to Disabled. Every IPX interface in the router configuration uses the same global host number, which is one of the following:

- A number derived from the router backplane
- A number that you enter into the Router Host Number parameter field

You specify the source for the host number by entering a host number in the Router Host Number field of the IPX Global Parameters window. (If you do not enter a number, the router derives the internal serial number from the router backplane, and uses this number for the global host number.)

Site Manager: Multiple Host Address Enable parameter: page A-10
Site Manager: Host Number (hex) parameter: page A-24

IPX Host ID Numbers

On Bay Networks routers, the IPX host ID number maps to a physical data link layer address (on a specific circuit or physical interface). An IPX logical interface can listen at this address and capture frames transmitted by nodes compatible with IPX on the local data link.

Figure 3-2 illustrates this concept in a Bay Networks router that has two IPX logical interfaces, each one configured on a different physical circuit.

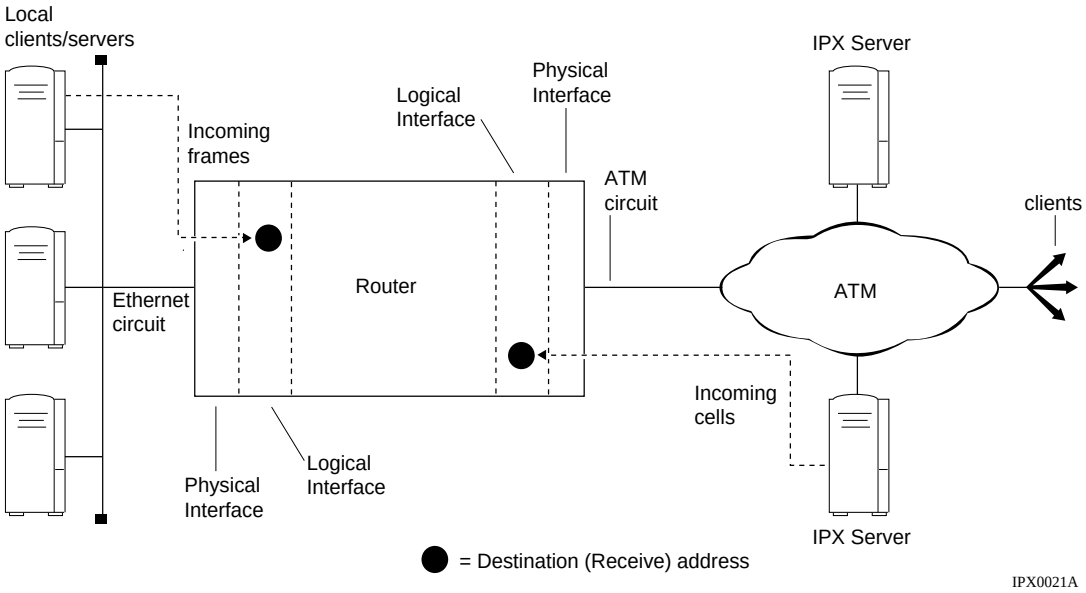

Figure 3-2. Frames Received at a Logical Interface

IPX compatible nodes on the same logical network and locally attached physical segment must use the host ID number of the IPX logical interface as a data link layer destination address, through which any transmitted frames can ultimately reach their target client or server applications.

Because an IPX logical interface can receive and send data, the host ID also identifies a source data link layer address from which the interface can send frames to nodes compatible with IPX anywhere else in the same IPX internetwork.

Figure 3-3 illustrates this concept in a Bay Networks router configured with two IPX logical interfaces, each one on a different physical circuit type.

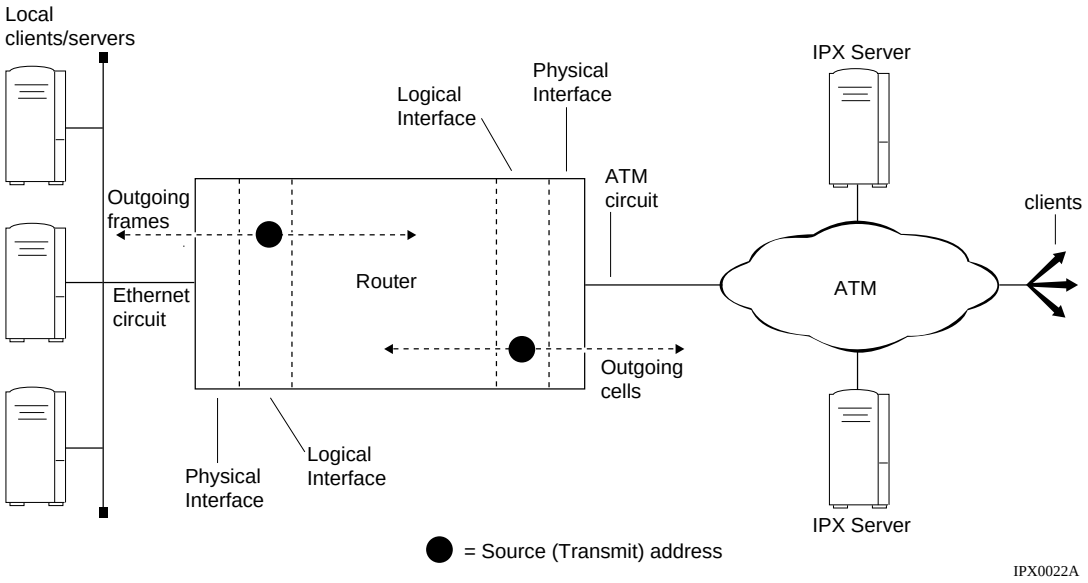

Figure 3-3. Frames Issued from a Logical Interface

Setting a Host ID Number for IPX on a Token Ring Circuit

In a configuration with IPX logical interfaces on a Token Ring circuit, the data link layer address is a MAC-layer address.

In Bay Networks routers, you set the MAC-layer address for the circuit and the host ID number for the IPX interface independently. However, the host ID number for every IPX logical interface on a given Token Ring circuit must be identical to the MAC address set for that circuit. Otherwise, the logical interface would send frames that contained an incorrect source MAC address, or the interface would listen for frames at the wrong MAC address.

Site Manager: Router Host Number (hex) parameter: page A-11

Token Ring MAC Address Selection

For Token Ring circuits, you can select the means by which the router determines the MAC address for a circuit by setting the MAC Address Select parameter on the Token Ring configuration window for that circuit to one of the following:

- PROM. (This is the default setting.) The circuit retrieves the MAC address that is stored in a PROM on the supporting link module.
- BOXWIDE. The circuit generates a MAC address based on the serial number of the backplane of the router.

Caution: The IPX boxwide host address and the Token Ring MAC address must agree when the Multiple Host Address parameter is disabled.

- CNFG. You can configure a MAC address.

Caution: Changing the setting of the MAC Address Select parameter to accommodate IPX configuration requirements can affect other protocol interfaces (for example, LNM Servers or IP) configured on the same circuit(s) with IPX. If necessary, make adjustments to the parameter settings of any such (non-IPX) interfaces configured on the router.

If you choose the CNFG option of the MAC Address Select parameter, you must subsequently enter a valid MAC address in the MAC Address Override parameter. You must repeat this procedure on any Token Ring circuit for which you choose CNFG (user configured) as the source for the MAC address assigned to the individual physical circuit. For instructions on how to set the MAC Address Select and MAC Address Override parameters, see *Configuring Line Services*.

Customizing IPX

After selecting a circuit and configuring the associated LAN parameters, your circuit will be operational. The default values set by the Site Manager for the remaining parameters will apply to most environments. However, if you want to configure a circuit in a particular way, refer to Chapter 5.

Chapter 4
Customizing IPX for WAN Media

You can use IPX services over either a LAN or a WAN. This chapter discusses issues related specifically to customizing IPX for use over a WAN. For information specific to using IPX over a LAN, refer to Chapter 3. For information on how to customize IPX features for use on both a LAN and a WAN refer to Chapter 5.

IPX over WAN Media

You can establish an IPX connection over any of the WAN media types supported by Bay Networks IPX router (refer to Table 2-2). The choice of protocols depends on the type of connection and what you want the protocol to do.

The WAN protocol PPP uses the IPXCP protocol (RFC 1552). IPXCP supports the routing of IPX packets over wide-area links that support only the Point-to-Point Protocol. IPXCP is a data link protocol that is part of PPP. To enable IPXCP, you must first configure the interface to support PPP. For instructions on how to do this, refer to *Configuring PPP Services*.

For the ATM, SMDS, X.25 PDN, X.25 Point-to-Point, and Bay Networks Point-to-Point protocols, once you choose the protocol, only one encapsulation method is allowed for all WAN protocols.

For the Frame Relay and PPP WAN protocols, you can optionally run IPXWAN (RFC 1634).

Note: Use IPXCP or IPXWAN when you want the routers to negotiate the options required for communication over the WAN link. Alternatively, you can explicitly specify the values for the WAN link without using either IPXCP or IPXWAN, as long as you ensure that what you configure at each end of the link is compatible.

Using IPXCP and IPXWAN

Incorporating IPXWAN in the Bay Networks router provides the following benefits:

- Adherence to RFCs 1362 and 1634 IPXWAN protocols developed by Novell
- A common link negotiation method for WAN media (Frame Relay and PPP)
- Interoperability with other routing vendors (for example, Novell)
- A standardized means for tick-based routing over WAN media

If you configure a local and a remote node to support both IPXCP and IPXWAN, IPXCP always runs first. After the router completes IPXCP negotiation, it discards all IPXCP-negotiated options, and IPXWAN runs. Refer to “Assigning a Unique Network Number” on page 4-4 for more information about specifying support for IPXCP and IPXWAN.

Running IPXWAN over PPP

IPX uses PPP when operating over point-to-point synchronous networks. With PPP, establishing a connection means that the IPX Network Control Protocol (NCP), IPXCP, reaches the Open state.

PPP lets either side of a connection stop forwarding IPX packets if one end sends an IPXCP Terminate request. When a router detects this, it immediately reflects the lost connection in its routing information database.

Running IPXWAN over Frame Relay Permanent Virtual Circuits

Each IPX packet is encapsulated in a Frame Relay frame. When an interface is restarted, IPXWAN exchanges begin immediately over active, direct mode Frame Relay PVCs (those that have remained active before and after restart).

- When a router detects that a direct mode Frame Relay PVC has gone from an inactive to an active state, the connection is established; and IPXWAN packet exchange over this newly activated connection begins.
- When an active PVC becomes inactive, the router reflects the lost connection in its routing information database.

Note: For IPX, you can use Frame Relay's direct, group, or hybrid mode. For IPXWAN, only direct mode is valid. In Frame Relay, direct mode is a point-to-point connection. Frame Relay group mode (or hybrid mode) involves a point-to-multipoint connection.

Negotiating an IPXWAN Connection

Establishing an IPXWAN connection involves negotiating which router will be the master. Being the master does not imply any special privileges; it simply indicates which router is the requestor in the ensuing request/response exchanges. A router retains its role -- master or slave -- for the remainder of the IPXWAN exchanges. The following options are determined after successful negotiation by the IPXWAN protocol:

- WAN link delay used in tick-based routing across the WAN link
- Network number for the WAN link
- Routing protocol to be implemented over the WAN link

Configuring an IPX Service to Run over a WAN

When you configure an IPX service to run over a WAN, you need to make sure the following parameters have the appropriate settings on the IPX Configuration window.

- Configured Network Number (required if IPXWAN is disabled)
- RIP/SAP

- Circuit Index
- IPXWAN
- Common Network Number (required for IPXWAN)
- Negotiated Protocols (required for IPXWAN)

In addition to parameters you set on the IPX Configuration window, you must also set the following parameters on the IPX Global Parameters window.

- Enable
- Multiple Host Address Enable
- Router Name (required for IPXWAN)
- Primary Network Number (required for IPXWAN)

If you are running IPX over an ATM network, you should set the Host Number on the IPX Interfaces window

Assigning a Unique Network Number

When you initially add an IPX interface to the router configuration, you must enter the network number of the IPX network segment associated with that interface. You should specify a network number of zero if you are configuring interfaces with unnumbered point-to-point links, and if IPXWAN is not enabled.

When the router recognizes a network number of zero, it knows that a lower protocol layer (IPXWAN or IPXCP) on the same circuit must negotiate with the remote IPX host for the network number of the intervening WAN segment.

Site Manager: Configured Network Number (hex) parameter: page A-2

Enabling RIP and SAP on an Interface

The default for this parameter depends on the protocol you are using. If you selected RIP/SAP, both RIP and SAP are automatically enabled. You can disable both RIP and SAP, or you can disable and re-enable just RIP or just SAP.

Site Manager: RIP/SAP parameter: page A-3

Identifying a Circuit

The Site Manager automatically assigns a circuit identifier to each circuit that you create on an IPX router. You can assign a specific circuit identifier, if necessary.

Site Manager: Circuit Index parameter: page A-4

Entering an IPX Host ID Number for IPX over ATM

On Bay Networks routers, the IPX host ID number maps to a physical data link layer address (on a specific circuit or physical interface). An IPX logical interface can listen at this address and capture frames transmitted by nodes compatible with IPX on the local data link.

Figure 4-1 illustrates this concept in a Bay Networks router that has two IPX logical interfaces, each one configured on a different physical circuit.

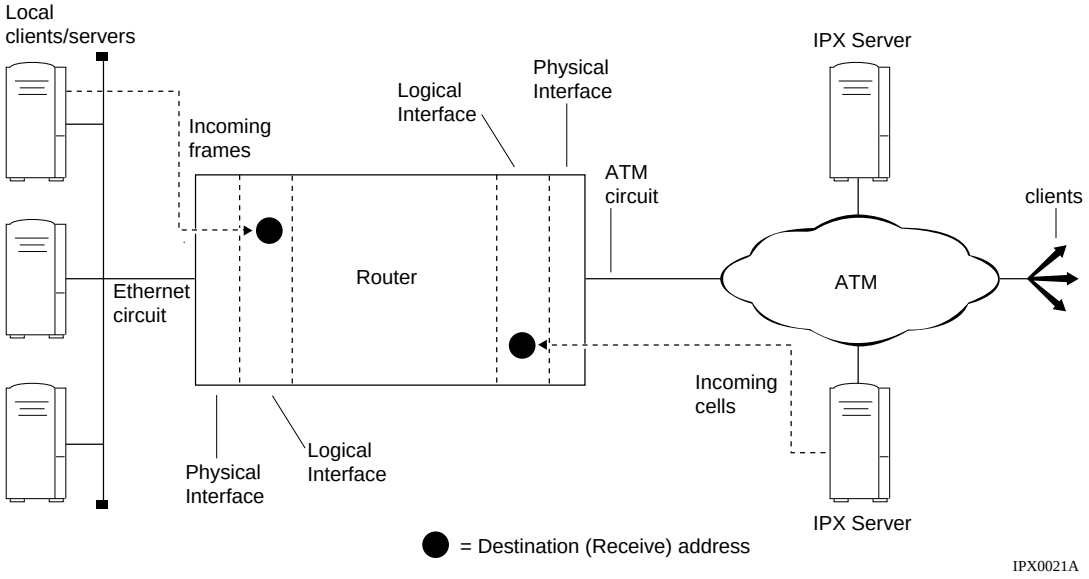

Figure 4-1. Frames Received at a Logical Interface

Figure 4-2 illustrates this concept in a Bay Networks router configured with two IPX logical interfaces, each one on a different physical circuit type.

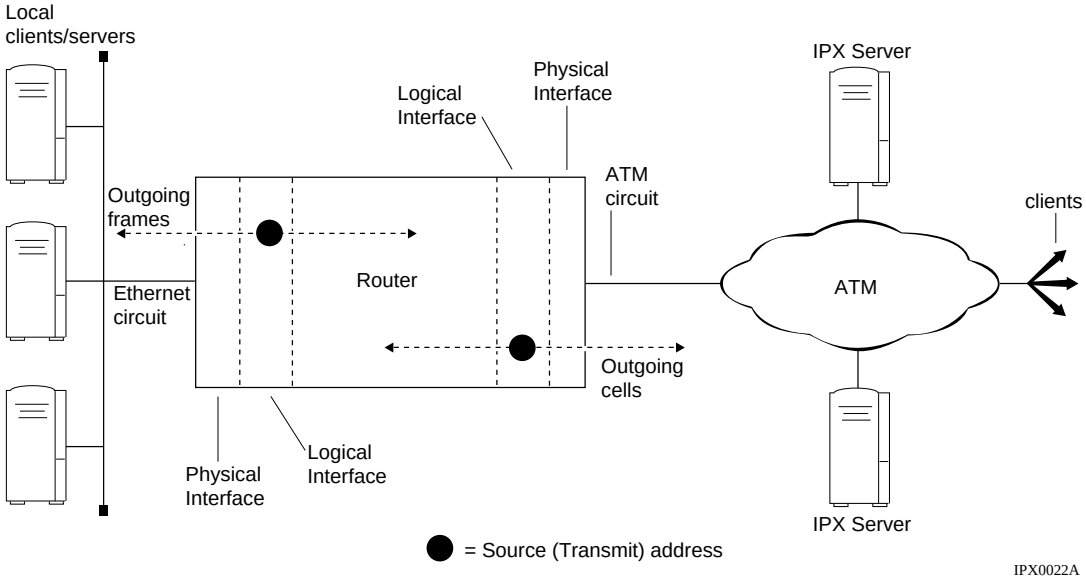

Figure 4-2. Frames Issued from a Logical Interface

To establish an IPX connection over an ATM network, you must assign a unique host ID number to the ATM interface that is running IPX. To assign a number, you can either

- Enter a value using the Host Number parameter
- Specify that the global MAC address be used for the host ID by disabling the Multiple Host Address Enable parameter

Site Manager: Router Host Number (hex) parameter: page A-11 Site Manager: Multiple Host Address Enable parameter: page A-10

Enabling IPXWAN for an Interface

If you want to run the IPXWAN protocol over a WAN, you should enable IPXWAN on the IPX interface. Enabling IPXWAN provides a common link negotiation method and a standard means for tick-based routing for WAN media.

Site Manager: IPXWAN parameter: page A-5

Assigning a Primary Network Number

Like Novell routers and servers, a Bay Networks router running the IPXWAN protocol implements a global “internal network,” to which you must assign a network number called the Primary Network Number (PNN). IPXWAN requires the PNN to determine whether the local or the remote router on a WAN link serves as the master or slave during the IPXWAN negotiations. The router with the higher PNN serves as the master.

Site Manager: Primary Net Number (hex) parameter: page A-8

Assigning a Common Network Number

The Common Network Number (CNN) is an IPX network number that is available for assignment to the WAN link. You specify a CNN that IPXWAN, running on the interface, can assign to the WAN link. To assign its CNN, the router must serve as the master during the IPXWAN negotiations. To specify a CNN, use the IPXWAN Common Network Number Parameter in the Configuration Manager IPX Interfaces window. Refer to page A-21 for more information on how to access this window.

All values between 0x00000000 and 0xFFFFFFFD, inclusive, are valid CNN values. Never use the values 0xFFFFFFFE or 0xFFFFFFFF as CNN values; these values are reserved.

Site Manager: Common Network Number (hex) parameter: page A-5

Entering a Router Name

Every IPX router can have a router name. During IPXWAN negotiations, the local and remote routers provide each other with their respective router names. Once the link is established, the name lets a router know whom it is connected to. Router names are particularly helpful for network management purposes. A symbolic name, such as “printserv,” has more meaning than just a string of digits.

The router name can be up to 47 characters long and can contain the characters A through Z, a through z, 0 through 9, and the special characters underscore (_), hyphen (-), slash (/), and at (@) signs. Some valid names include

- AAaabbBBxxXXXS/1234
- myrouter@first_floor
- Chicago_office

Site Manager: Router Name parameter: page A-7

Indicating the Protocol Negotiated for an Interface

When you specify an IPXWAN interface on a circuit, you must indicate the protocol negotiated for this interface. The choices are RIP and Unnumbered RIP.

Site Manager: Negotiated Protocol(s) parameter: page A-6

Sample IPXCP and IPXWAN Configurations

Figure 4-3 shows a local router communicating with a remote router using IPXCP over PPP, and the same local router communicating with a remote router using IPXWAN over Frame Relay.

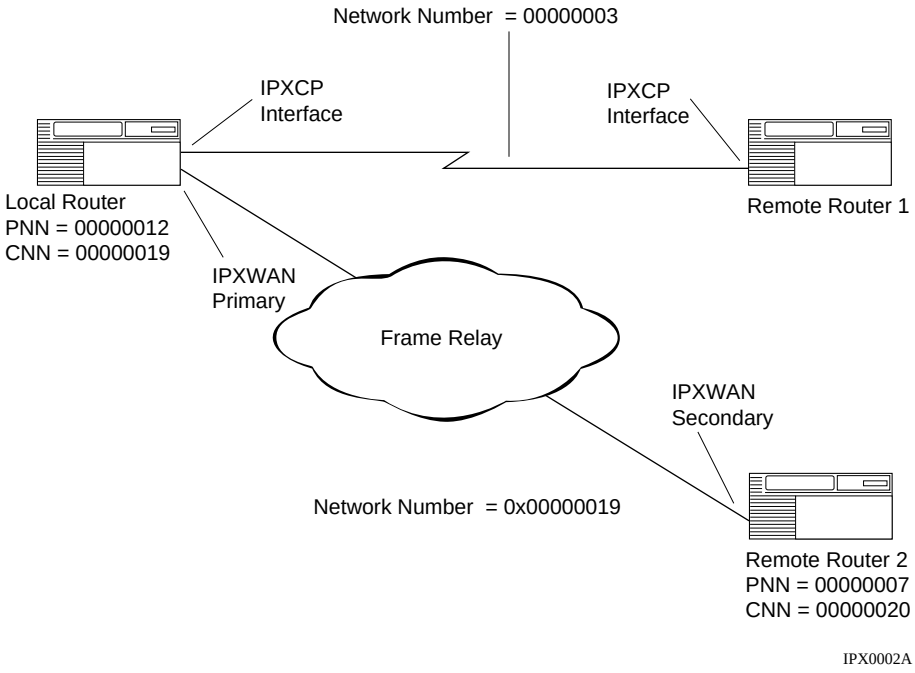

Figure 4-3. IPXCP and IPXWAN Configurations

IPXCP Link Negotiation

In Figure 4-3, the local router and Remote Router 1, both configured for IPXCP, negotiate a connection at the data link layer. Once the options are successfully negotiated, the IPXCP interfaces in both the local router and Remote Router 1 must agree on a unique network number. When you initially configure an IPXCP interface, you assign an IPX network number to that interface. The routers select the higher of the two IPX network numbers. See *Configuring PPP Services* for instructions on configuring the IPX network number for an IPXCP interface.

Note: For PPP communication between a Bay Networks Version 7, 8, 9, 10, or 11 IPX router and a Bay Networks Version 5 IPX router (or any other vendor's router that does not support IPXCP negotiations), you must manually configure the network number of the IPX interface on both routers.

IPXWAN Link Negotiation

The local router and Remote Router 2 are both configured for IPXWAN. When you initially configure an IPXWAN interface, you assign a Primary Network Number (PNN) to the router. The router with the highest PNN becomes the master during IPXWAN negotiations on that WAN link.

In Figure 4-3, the local router (PNN=00000012) is the master, and Remote Router 2 (PNN=00000007) is the slave. During the IPXWAN negotiations, both routers negotiate their link options. If successful, the CNN configured for the interface on the master becomes the IPX network number for the WAN link.

Once the IPXWAN negotiations are successful on the WAN link, each router connected on the link can advertise information in its routing/forwarding tables.

IPXWAN and IPXCP Link Configurations

Table 4-1 shows the various WAN protocol configurations likely to exist within local and remote IPX router interfaces. Find the configuration that applies to your situation, as indicated in the table, and read the corresponding description that follows.

Table 4-1. Configuration Table for IPX Over WAN Media

Local IPX Interface	Remote IPX Interface			
	IPXWAN with IPXCP	**IPXWAN but not IPXCP**	**PPP with IPXCP; no IPXWAN**	**PPP without IPXCP; no IPXWAN**
IPXWAN with IPXCP	Configuration 1	Configuration 2	Configuration 3	Configuration 4*
IPXWAN but not IPXCP	Configuration 2	Configuration 2	Configuration 4	Configuration 4
PPP with IPXCP; no IPXWAN	Configuration 3	Configuration 4	Configuration 3	Configuration 4
PPP without IPXCP; no IPXWAN	Configuration 4*	Configuration 4	Configuration 4	Configuration 4
* Bay Networks 11.00 to Bay Networks Series 5.*x* IPX Router Compatibility				

Configuration 1 (IPXWAN with IPXCP on Both Interfaces)

In this configuration, IPXWAN defers to IPXCP for link negotiation.

- IPXWAN negotiation supersedes IPXCP negotiation, regardless of whether IPXCP negotiation succeeds.
- If IPXWAN negotiates successfully, the IPX interface becomes active. If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines -- Configuration 1

- IPXCP -- Use the value zero for the IPX network number when configuring the local and remote Point-to-Point Protocol interface.
- IPXWAN -- Use a unique router name and Primary Network Number in the IPX Global Parameters window when configuring the local routers.

You must enable IPXWAN on the interface. You must also enter a unique Common Network Number for the IPX interface you just configured, except that the CNN can be zero when Unnumbered RIP is configured on both interfaces.

Site Manager: IPXWAN parameter: page A-5
Site Manager: Common Network Number (hex) parameter: page A-5

Configuration 2 (IPXWAN on Both Interfaces)

In this configuration, IPXWAN exclusively negotiates an IPX network number for the link. If IPXWAN negotiates successfully, the IPX interface becomes active. If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines -- Configuration 2

- IPXCP -- No configuration requirements.
- IPXWAN -- Use a unique router name and PNN in the IPX Global Parameters window when configuring the local and remote routers.

You must enable IPXWAN on the interface. You must also enter a unique Common Network Number for the IPX interface you just configured, except that the CNN can be zero when Unnumbered RIP is configured on both interfaces.

Configuration 3 (Only IPXCP on Both Interfaces)

In this configuration, IPXCP exclusively negotiates an IPX network number for the link.

- If IPXCP successfully negotiates the number, the IPX interface becomes active on the link.
- If IPXCP fails to negotiate a number, the IPX interface cannot become active.

Configuration Guidelines -- Configuration 3

- IPXCP -- Use any valid value for the IPX network number when configuring the local or remote PPP interface.
- IPXWAN -- No configuration requirements.

Configuration 4

In this configuration, the lower layer has no means of negotiating an IPX network number for the link. For this reason, you must manually configure the network number of the local and remote IPX interfaces to the same value.

Customizing IPX

After selecting a circuit and configuring the associated WAN parameters, your circuit will be operational. The default values set by the Site Manager for the remaining parameters will apply to most environments. However, if you want to configure a circuit in a particular way, refer to Chapter 5.

Chapter 5
Customizing IPX

This chapter explains how to customize IPX parameters to fit your environment. In most cases, after you add a circuit and supply the LAN or WAN parameters, you can leave the remaining parameters with the default values and begin sending packets over the network.

If you have a special configuration, use the information in this chapter to customize the following groups of parameters:

- Advanced global parameters
- Interface parameters
- Routing Information Protocol (RIP) parameters
- Service Advertisement Protocol (SAP) parameters
- Static service parameters
- NetBIOS static routing parameters
- Adjacent host parameters
- Dial-on-Demand parameters
- Dial optimized routing parameters
- Static route parameters
- Route filter parameters
- SAP filter parameters
- Service name filter parameters
- Source route bridge endstation support

Customizing Advanced Global Parameters

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. You can customize the parameters that affect all interfaces by modifying the values of the Advanced Global Parameters found on the IPX Advanced Global window.

Setting the Maximum Number of Paths

Specify the maximum number of paths allowed for a given network destination and routing method. Multiple paths to a given destination uses more memory than single paths, but gives you redundancy. Specifying multiple paths allows you to do load balancing (see "Specifying the Number of Maximum Path Splits" below).

Site Manager: Maximum Path parameter: page A-15

Selecting a Log Filtering Mode

You can filter out specified types of log message. For example, the default setting (Trace) filters out trace messages.

Do not change the default value of this parameter unless you are an expert IPX user. Changing the value of this parameter produces significant boxwide effects on memory allocation within the router, and these changes can significantly affect router performance.

If you are qualified as an expert user, enter a filtering mode that yields a level of performance most appropriate for network applications supported by this router.

Site Manager: Log Filter parameter: page A-15

Specifying the Number of Maximum Path Splits

You can specify the maximum number of equal-cost paths over which IPX will do load balancing to a particular destination. For example, if the maximum path splits is non-zero, and there are five equal-cost routes to a destination, IPX will distribute the packets over the five paths in a round-robin fashion.

Site Manager: Maximum Path Splits parameter: page A-15

Specifying the Maximum Number of Destinations

You can specify the maximum number of destinations (networks) for the router to learn. IPX uses this value to preallocate table sizes for forwarding and network tables. If you specify zero, the default value, IPX dynamically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory used by IPX, but it can also speed learning time for the router.

Site Manager: Destination Count parameter: page A-16

Entering the Maximum Number of Services

You can enter the maximum number of services for the router to learn. IPX uses this value to preallocate table sizes for service tables. If you specify zero, the default value, IPX automatically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory used by IPX, but it can also speed learning time for the router.

Site Manager: Service Count parameter: page A-17

Specifying the Granularity for Aging RIP and SAP Information

You can specify the granularity, in seconds, for aging RIP and SAP information. IPX checks whether any routes have timed out every *n* seconds, where *n* is the interval that this parameter specifies.

Site Manager: Aging Frequency parameter: page A-18

Specifying the Aging Pending Frequency

You can specify the number of routes and services to age (process) before pending. A higher number lets the aging process proceed more quickly.

Site Manager: Aging Pending Frequency parameter: page A-18

Enabling IPX Default Routing

You can globally enable or disable the use of the default route 0xFFFFFFFE for IPX routing.

- Enable -- Directs the router to use the default route (if one exists in its routing table) when it receives an IPX packet that does not contain a known IPX destination address within the IPX protocol header.
- Disable -- Forces the router to drop a packet whose destination address is unknown, even if a default route exists.

Site Manager: Default Route parameter: page A-19

Multipath Routing and Load sharing

You can include multiple next-hop destinations as active routes to a destination network. The IPX router can find out about multiple paths by either RIP packets or statically configured routes.

The router can forward packets to the multiple next-hop nodes concurrently by multiplexing frame transmissions over the multiple equal-cost paths in a cyclic sequence. This is referred to as *IPX multipath* or *IPX load sharing*.

Multipath Routing

Multipath is a “round-robin” or cyclic multiplexing mechanism. When multiple least-cost paths of equal tick delay and hop count exist between IPX source and destination networks, standard RIP operation uses only one of these routes. The multipath feature takes advantage of these multiple equal-cost routes and distributes the packet load among them, balancing the IPX traffic across these routes and maximizing internetwork performance. When you enable multipath routing, the IPX router diverts individual, consecutive frames destined for the same target network to separate IPX interfaces and their associated physical circuits. (Figure 5-1.)

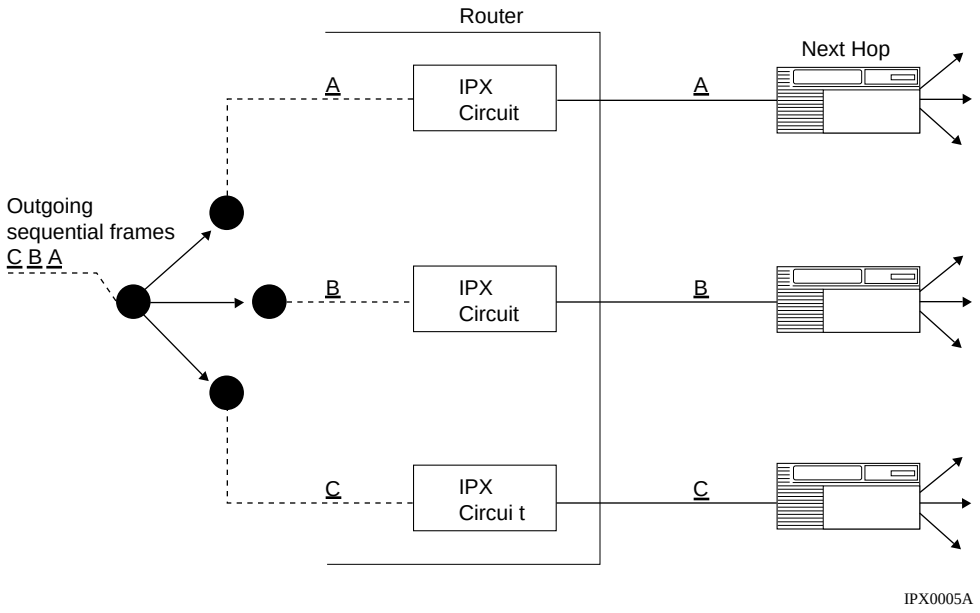

Figure 5-1. IPX Multipath

Because the IPX interfaces have duplex functionality, the router can also use multipath to collect frames received from separate IPX interfaces. The router operates this cyclic mechanism at a bandwidth significantly greater than a single IPX interface and its supporting physical circuit can support. The result is that IPX frames flow over multiple parallel LAN or WAN routes concurrently, in effect, aggregating the bandwidth supported by the parallel routes. Each line shares $1/n^{th}$ of the total load (where n is the number of equal-cost parallel routes or paths to the destination network).

You set the maximum number of paths by means of the Maximum Path parameter.

Site Manager: Maximum Path parameter: page A-15

Any setting greater than 1 engages the multipath mechanism. Figure 5-2 is an example of equal, least-cost, parallel routes used in IPX multipath routing.

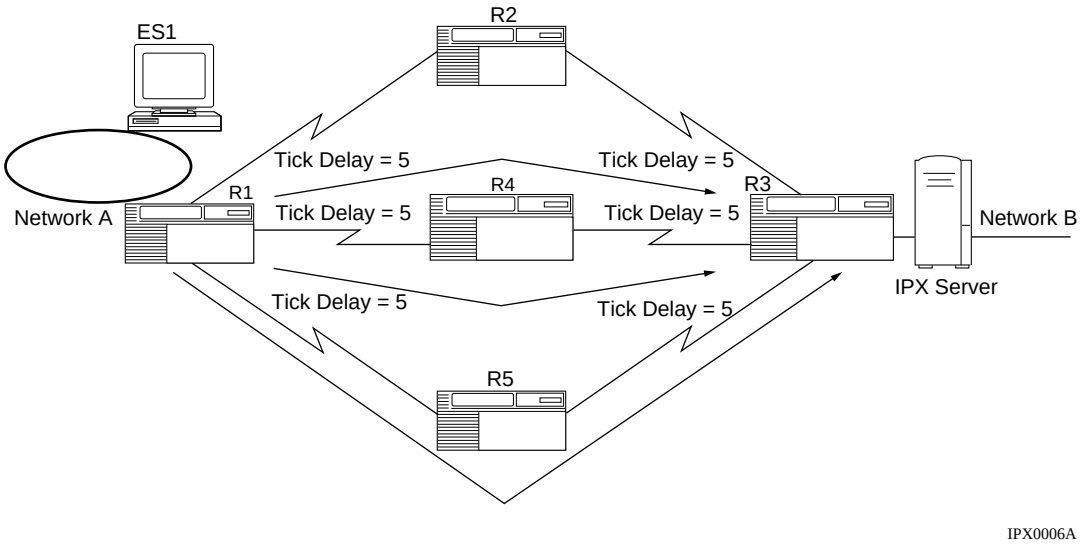

Figure 5-2. IPX Multipath Routing -- Equal Least-Cost Routes

Because of the round-robin algorithm, IPX packets that belong to the same data stream may require resequencing at their ultimate destination. Therefore, higher-layer protocols such as SPX must be used in both source and destination IPX routers to provide packet resequencing. To derive maximum benefit from this feature, the source and destination nodes should support burst-mode operation.

Load Redistribution and Rerouting

If the router with multipath enabled detects a failure, it temporarily redistributes the IPX traffic among the remaining active original least-cost routes. When the router learns (through RIP packets) of the existence of an alternative least-cost route, or when the failed route returns, IPX multipath returns to its original IPX traffic distribution.

Multipath Route Precedence/Priority

The multipath mechanism generally uses the best path first. However, when two equal-cost paths exist, multipath uses the following priority scheme for route selection:

1. Direct routes (paths to other routers on a segment directly attached to the local router)
2. Routes learned via RIP
3. Statically configured routes

Multipath Configurations

You can establish equal-cost multipath routes over LAN or WAN segments to support IPX traffic between routers, and between routers and servers. The slower the interconnecting LAN or WAN links, the more difference using multipath will make in client/server throughput.

Multiline Circuits

The multiline circuits feature allows a single circuit to be composed of up to 16 individual synchronous network data paths. Multiline circuits support provides a level of redundancy not available through conventional single-line circuit configurations. The multiline circuits feature ensures routing circuit availability in the event of a single data path failure.

Equally important, the multiline circuits feature provides increased bandwidth between two sites without the circuit management complexities associated with multiple circuits. Once you've configured and enabled the circuit, the use of multiple data paths to form a single circuit is transparent to both network management and the end-user community.

Multiline circuits provide the following methods for transmitting traffic over their data paths:

- Address-based data path selection
- Random data path selection

Address-based data path selection determines the path a packet traverses based on its source and destination addresses. Once a path has been established for a given address pair, subsequent packets will follow the same path. This ensures that packets will be received in the order in which they were sent. This is essential for protocols that cannot tolerate receiving packets out of order.

Random data path selection determines the path a packet traverses based on a randomly assigned number that corresponds to a particular data path of the multiline circuit. This algorithm avoids congestion by providing even distribution across multiple data paths. Unlike address-based selection, random data path selection does not guarantee the sequence of packets as they are received at their destination. Consequently, random data path selection is intended for use with protocols whose upper layers provide resequencing techniques.

Note: For Bay Networks software Version 7.60 and later, support of multiline circuits is compatible with the Version 5.*x* "Circuit Groups" feature, except that Version 7.60 and later software does not support LAN media multiline circuits grouping. Multiline circuits can be configured using only synchronous interfaces data paths, including HSSI. All data paths must incorporate the same encapsulation method, Maximum Transfer Unit (MTU), and effective bandwidth.

The differences between multiline circuits and IPX multipath are the following:

- Multiline circuits operate across point-to-point links between two Bay Networks routers, while IPX multipath operates across a random topology (both LAN and WAN).
- Multiline is protocol-independent, while IPX multipath is IPX-based.
- Multiline circuits require WAN links of equal bandwidth on which to distribute IPX traffic, while IPX multipath supports links of varying speeds.
- Multiline circuits do not support the adoption of alternative links when WAN links fail.

Selecting the GNS Response Mode

When a server responds to a get_nearest_server request, it can either sort through all server names alphabetically or select the last server learned.

Site Manager: GNS Response Mode parameter: page A-20

Customizing Interface Parameters

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. These interface parameters determine how IPX behaves on individual router interfaces. You can customize the parameters that belong to a specific interface by modifying the values of the Interface Parameters found on the IPX Interface window.

Enabling IPX Routing on an Interface

After you add an interface to a circuit, you can enable or disable IPX routing on this interface. IPX routing is automatically enabled on an interface.

Site Manager: Enable parameter: page A-22

Entering a Symbolic Name for an Interface

You can specify a symbolic name for an interface on a server. For example, first_floor_printer.

Site Manager: Name parameter: page A-22

Assigning a Host Number to an Interface

If you enable Multiple Host Address Enable and want to accept the PROM-based default setting for the MAC Address Select circuit parameter, this IPX interface adopts a host number based on the MAC address of the underlying circuit. In this case, a PROM on the circuit supplies the number for the MAC address of the circuit and the host number of the interface.

You can enter a host number for this interface when:

- Multiple Host Addressing is enabled
- You do not want to accept the PROM-based (default) setting for MAC Address Select
- The circuit type supports only selective mode of operation (such as with Ethernet circuits)

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains effective for all other interfaces configured on the same circuit.)

Site Manager: Host Number (hex) parameter: page A-24

Enabling Source Routing for an Interface on a Token Ring Circuit

You can enable or disable source routing for an interface on a Token Ring circuit.

Site Manager: TR End Station parameter: page A-25

Entering a Broadcast Address

You can enter a WAN broadcast address for an IPX interface. The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a WAN broadcast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

You can leave this parameter blank to accept the default value, or enter a WAN broadcast address to send all broadcast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all broadcast traffic through all logical connections associated with the IPX interface you are configuring. Broadcast traffic includes RIP and SAP broadcasts.

Site Manager: FR Broadcast (hex) parameter: page A-27

Entering a Multicast Address

You can enter a WAN multicast address for an IPX interface. The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a multicast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

You can leave this parameter blank to accept the default value, or enter a WAN multicast address to send all multicast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all multicast traffic through all logical connections associated with the IPX interface you are configuring.

Site Manager: FR Multicast (hex) parameter: page A-27

Responding to IPX Watchdog Packets

You can enable or disable a router from responding locally to broadcast IPX watchdog packets on behalf of clients that use dial-in connections. You should enable local watchdog packet acknowledgment to reduce WAN costs by using dial-on-demand routing. SPX Keep Alive Spoofing is introduced in version 11.0 and is enabled when Watchdog Spoofing is enabled.

Site Manager: IPX Watchdog Spoofing parameter: page A-28

Setting Delay Time

You can specify the length of time, in microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit, if the circuit is free of other traffic.

Site Manager: Delay parameter: page A-28

Specifying Throughput

You can specify the amount of data, in bits per second, that can flow through an IPX circuit if the circuit is free of other traffic.

Site Manager: Throughput parameter: page A-29

Setting Stabilization Timer Delay

You can set the amount of time, in seconds, that RIP/SAP waits before sending out initial route information when the circuit first becomes active. The more routes that you expect a router to handle or the more dynamic the network is, the higher you should set this value to allow the router enough time to assimilate incoming routes before it sends out an initial update on a circuit.

Site Manager: Stabilization Timer Delay (secs) parameter: page A-28

Handling Packets Associated with Upper-Layer Protocols

The router encapsulates, within the data field of an IPX packet, any packets associated with Novell's upper-layer protocols. The structure of a packet, as well as the source and destination socket numbers contained in that packet, identify the protocol type associated with that packet; for example, Service Advertising Protocol and Routing Information Protocol. The upper layer services are

- SPX
- NCP

Bay Networks router software lets you select the basis on which an IPX router makes its routing decisions — on the number of *ticks* or the number of *hops* required to reach a given destination network. The IPX routing software also provides the following services over LAN and WAN media:

- Multipath routing and load sharing
- Split Horizon capability
- NetBIOS all-networks-broadcast packets (Type 20 packets)
- Source routing and endstation support
- IPX ping capability

The following sections describe how Bay Networks routers support these services.

The Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) enables workstations and routers to exchange route information and to establish the route to each network with the fewest hops and shortest delay.

Each IPX router maintains a route table. The route table contains the following information about every network in the IPX network topology:

- The network address.
- The number of ticks (units of delay time) to that network. (A tick is equal to about $1/18^{th}$ of a second. The number of ticks to a network is the *tick cost* for that route.
- The number of hops to that network. (A hop is an adjacent router; the number of hops is equal to the number of adjacent routers that a packet must traverse to reach another network segment.)
- The address of the next-hop node to which the local router forwards packets on their way to another destination network.

Routers maintain route tables by exchanging RIP request and response packets. A RIP request packet specifies the destination network. A RIP request packet can be

- A general request broadcast by a router to retrieve the fastest route to all known networks on an internetwork. The value 0xFFFFFFFF in the network address field indicates that the packet is a general request.
- A specific request broadcast by a workstation or router to determine the fastest route to a particular network. One or more network addresses (excluding an address of all Fs) in the network address field indicates that the packet is a specific request.

Routers issue RIP response packets. RIP response packets contain the network number and the number of hops and ticks required to get to the network. A RIP response can be one of the following types:

- A response to a request.
- An informational broadcast from a router issued at regular intervals (by default, every 60 seconds).
- An informational broadcast when a change occurs in the routing table. Examples of changes in the routing table are tick or hop changes, timing out of routes, and the addition of routes to networks to the table.

- An informational broadcast when an interface initializes or performs an orderly shutdown procedure.

Each RIP packet can contain up to 50 route updates. To reduce traffic, RIP broadcasts are limited to a router's immediate segments and are not forwarded by receiving routers.

Note: The IPX router learns WAN addresses from RIP and SAP broadcasts received over WANs (Frame Relay, SMDS, ATM). The router stores IPX address/WAN address pairs for future use as next-hop destinations.

Enabling RIP on the Router

You can enable or disable RIP on a circuit. By default RIP is not enabled on the router unless you selected RIP/SAP on the Select Protocols menu when you first started IPX.

If you enable RIP on a circuit, a route filter can still prohibit the interface from updating its internal routing tables. See "Using IPX Route Filters," later in this chapter.

If you do not configure RIP for a WAN interface, you must configure adjacent hosts for all transmission paths to nodes adjacent to Frame Relay, ATM, or SMDS circuits when you configure an IPX interface. You must then configure static routes that use the adjacent hosts to reach next-hop routers. Refer to the descriptions of adjacent hosts and static routes in this chapter for more information on these features.

Site Manager: Enable parameter: page A-35

Choosing the Routing Method

You can specify a method for making IPX "best-route" decisions for all slots, based on time delays (ticks) incurred or hops encountered for packet delivery.

The router can assess the time delay in one of the following ways:

- *Number of RIP timer ticks* -- the amount of time, expressed in ticks, that a packet requires to reach another network segment. (Each RIP timer tick equals about 1/18th of a second. The maximum configurable number of ticks is 65,534 ticks, multiplied by 1/18th of a second = 3600 seconds, or 60 minutes.
- *Number of hops* -- the number of router hops a packet must traverse to reach a network segment. The maximum number of hops is 15.

We recommend using the default (tick-based) method. Note that every node on the network must use the same routing method.

Site Manager: Routing Method parameter: page A-14

Setting a Cost for an Interface

You can set the cost (number of ticks or hops) for an interface. The value you enter depends on whether you selected hops or ticks for the RIP Method parameter.

By configuring an interface's cost you can select the route you want to use, rather than letting the router select the route. For example, two routes go to the same destination. Route A has a tick cost of 2; Route B has a tick cost of 3. Because Route A has the lower tick cost, the router selects it as the "best route" to the destination. If you want traffic to go over Route B, you can set the tick cost of Route A to 4, which then forces traffic to go over Route B.

Using configurable RIP interface tick values, IPX routing decisions can be based on tick values that you define. This allows the implementation of tick-based routing over non-IPX WAN links (for example, HDLC encapsulation), letting you optimize IPX network performance.

In Figure 5-3, for example, traffic generated by End System 1 (ES1) on Network A is directed to the IPX Server ES2 on Network B over Interface 2 (route of least tick delay, per RIP specification). However, other protocols such as IP, AppleTalk, and OSI will most likely select this route as the least-cost path between Network A and Network B, as well. Consequently, traffic congestion over this route may preclude it from being the most efficient path between these two network segments.

By implementing the Configurable RIP Interface Tick parameter, Interface 1 on Router 1 can be assigned a lower tick value than Interface 2, so that IPX traffic is routed through Interface 1. This lets you maximize IPX internetwork performance between Networks A and B, even though it traverses two T1 lines instead of one.

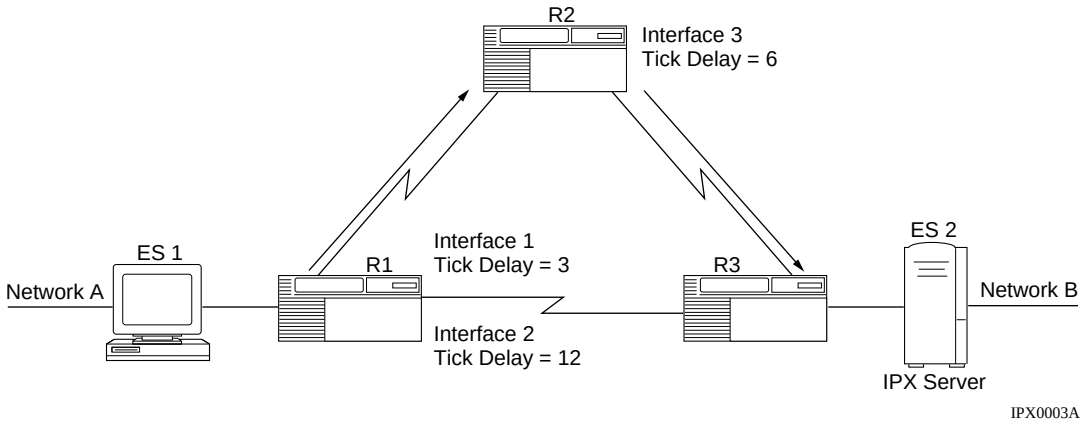

Figure 5-3. IPX Configurable RIP Interface Cost

You can set the cost (number of ticks or hops) for an interface. The cost is added to route information learned on this interface through RIP and is included in subsequent RIP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.

Site Manager: Cost parameter: page A-23

Specifying the Maximum Number of Hops

You can specify the maximum number of hops an IPX packet may take to reach its destination. In the case of RIP, every node in the network should use the same Maximum Hops parameter value.

Site Manager: Maximum Hops parameter: page A-16

Indicating the Number of Next-Hop Hosts

You can enter the maximum next-hop hosts for the router to learn. IPX uses this value to preallocate table sizes for host tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.

Site Manager: Host Count parameter: page A-17

Enabling RIP Listen and Supply Functions

The IPX router lets you enable the RIP listen and supply modes for each IPX interface. When you enable the listen mode, the IPX router learns routes received in RIP updates from neighboring routers. When you enable the supply function, the IPX router transmits RIP periodic and triggered updates to routers in adjacent networks.

When you enable both the listen and supply mode, the IPX router performs both the listen and supply mode functions described above.

Site Manager: Mode parameter: page A-35

Determining the Pace of RIP Packets

The RIP pace determines the frequency, in packets per second, at which RIP sends out packets on a circuit. By default, RIP sends out 18 packets per second on a circuit.

If you enter a value of zero, there is no limit on the pace.

Site Manager: Pace parameter: page A-36

Configurable RIP Timers

You can extend the standard 60-second IPX periodic RIP advertisement interval. You configure the interval by specifying the value of the Update Interval parameter, and the multiplier by specifying the Age Multiplier parameter. By default, the age-out time is three times the standard 60-second RIP advertisement update interval, or 180 seconds.

Site Manager: Age Multiplier parameter: page A-36
Site Manager: Update Interval (sec) parameter: page A-36

Configuring RIP timers can reduce IPX RIP overhead and enhance bandwidth availability. Furthermore, you can eliminate periodic RIP advertisements by setting the configurable RIP timer to zero; thus, only RIP updates triggered by changes in the internetwork topology will be propagated.

To ensure proper RIP operation, all configurable RIP timers must be set at equal advertisement intervals on all router interfaces attached to common IPX network segments.

Note: While you can set configurable RIP timers on any Bay Networks router interface, do not use them on LAN interfaces, because IPX servers do not allow configuration of update timers (with internal routers). As a result, IPX servers will by default purge RIP entries after 180 seconds if they have not received any updates within this 180-second period.

For example, in Figure 5-4, if Router R1 is configured to issue periodic RIP advertisements every 240 seconds over Interface 1 and Router R2 is configured to issue advertisements per the IPX standard (every 60 seconds) over Interface 2, then Router R2 will purge RIP entries learned through Interface 2 every 180 seconds and reinstate them 60 seconds later when it receives a periodic RIP advertisement from Router R1. More critically, Router R2 will issue triggered RIP updates through Interface 3, propagating these unnecessary changes throughout the internetwork behind Router R2.

Setting the configurable RIP timers at 240 seconds on both Interface 1 on Router R1 and Interface 2 on Router R2 ensures proper RIP operation, because RIP entries are not purged unless an update for a particular entry is not received within a 720-second interval (3 * 240 seconds).

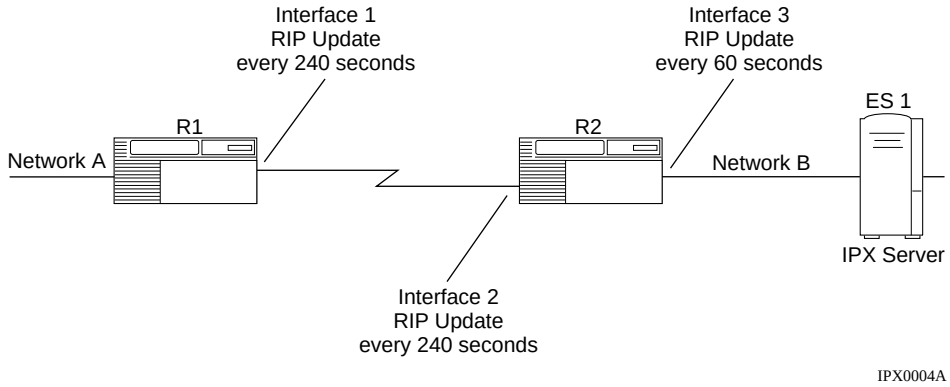

Figure 5-4. IPX Configurable RIP Timers

Taking into account the fact that IPX Server ES1 (with an internal router) on Network B expects periodic RIP advertisements every 60 seconds, Router R2 continues to issue RIP advertisements out its LAN interface (Interface 3) per the IPX specification, reconciling the fact that periodic RIP advertisements through Interface 1 are received every 240 seconds.

Should you decide to disable the periodic transmission of RIP updates, RIP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards.

The combination of the update interval and age multiplier should be the same for all systems on a network segment.

Adjusting the RIP Packet Size

By default the size of a RIP update packet is 432 bytes. You should leave the RIP packet size at the default level unless you have a specific reason for specifying a different size packet. If you must change the packet size, the packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

Site Manager: Packet Size parameter: page A-37

Enabling Multicast Transmission of RIP Packets

By default, the IPX router broadcasts RIP packets. If you enable this feature, use the Multicast Address parameter to specify the multicast address.

Site Manager: Use Multicast parameter: page A-37
Site Manager: FR Multicast (hex) parameter: page A-27

Configurable Split Horizon

The Split Horizon algorithm is part of the Novell specification for the IPX protocol. Its purpose is to prevent circular routes and reduce network traffic. The Bay Networks implementation of Split Horizon excludes RIPs and SAPs learned from a neighbor when forwarding RIP and SAP updates to that neighbor. Split Horizon is enabled by default for each interface. You can enable or disable Split Horizon when you configure the IPX RIP Circuit in the Configuration Manager.

Fully Meshed Networks

A fully meshed network is a WAN in which all nodes have a logically direct connection to each other. Figure 5-5 shows a sample fully meshed network with split horizon enabled.

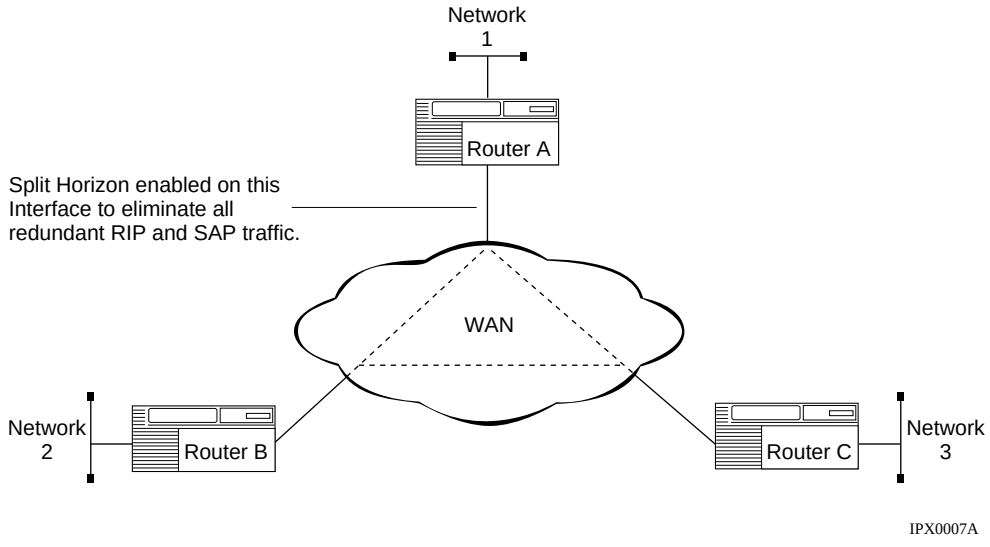

Figure 5-5. Split Horizon Enabled in a Fully Meshed Network

Nonfully Meshed Networks

A nonfully meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes. In a star or nonfully meshed Frame Relay or X.25 PDN topology, you may need to disable Split Horizon on certain interfaces so the routers can learn about other networks.

Caution: We advise you not to disable Split Horizon unless it is absolutely necessary. Doing so can result in a significant increase in network traffic.

Figure 5-6 shows a sample nonfully meshed network with Split Horizon disabled.

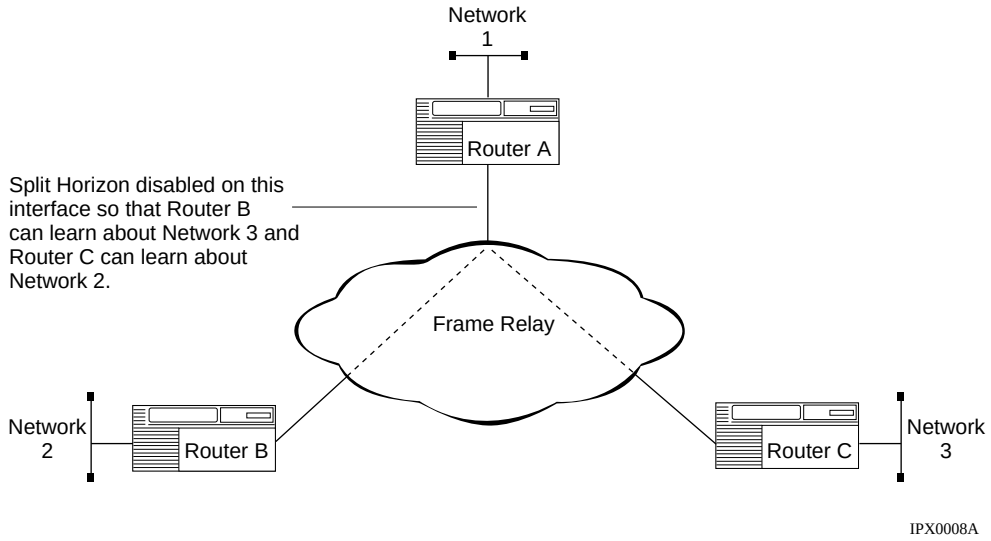

Figure 5-6. Split Horizon Disabled in a Nonfully Meshed Network

If you disable IPX Split Horizon, IPX sends all router services over nonfully meshed Frame Relay and X.25 topologies. For example, as shown in Figure 5-6, Router A propagates RIP and SAP packets pertaining to Router B to Router C, and vice versa. As a result, endstations on Network 2 can learn about Network 3, and endstations on Network 3 can learn about Network 2.

When Split Horizon is enabled for an interface, routes learned on that interface are not advertised out that interface.

Site Manager: Split Horizon parameter: page A-38

Updating Routers About a Failed Route

By default, when a circuit goes down on a router, the router immediately propagates this status change to other routers in the internetwork. This facilitates network traffic by letting routers know immediately about new or failed routes. When you disable the RIP Immediate Update parameter, other routers learn about such changes only at the next periodic update interval.

Site Manager: Immediate Update parameter: page A-38

Advertising Default Routes in RIP Packets

A RIP packet does not normally include a default route that exists in the routing table. Enable the Default Route Supply parameter if you want to advertise the default route in a RIP packet.

Site Manager: Default Route Supply parameter: page A-39

Accepting Default Route Information

When a router receives a RIP packet that advertises a default route, and if the Default Route Accept parameter is enabled on the receiving RIP interface, the default route is stored in the routing table.

Site Manager: Default Route Listen parameter: page A-39

Customizing SAP Parameters

NetWare network services use the Service Advertising Protocol to inform clients of their presence. NetWare services use the SAP identification broadcasting services to tell clients their name, type, and IPX address. The IPX address in a broadcast identifies a server's location in terms of network, host, and socket.

Site Manager: Enable parameter: page A-40

NetWare Directory Services (NDS) and SAP

Networks that implement NetWare 4.*x* use the NetWare Directory Services (NDS) to advertise services. NDS is a globally distributed network database that replaces the bindery used in NetWare versions earlier than 4.0. Workstations locate services by querying an NDS server. NDS maintains information about all network resources (users, groups, servers, file volumes, printers, and so on) in a hierarchical tree structure. Network resources can be organized in the tree independent of their physical location. Thus, network users can access any network resource they have rights to without having to know the exact location of the resource.

With NDS, users no longer need to log in or attach to specific servers. Instead, users can log in to the network and get access to all authorized network resources. NDS is compatible with bindery-based versions of NetWare through the bindery emulation feature of NDS.

The NDS server distributes the service information using direct unicast-based protocols instead of using broadcast-based SAP. Therefore, the use of SAP in an NDS network is greatly reduced. Even in a network that includes only NetWare 4.0 servers, however, clients still use SAP to locate the nearest NDS server at startup.

SAP and the NetWare Bindery (NetWare 3.*x* and Earlier)

Novell IPX routers running NetWare versions earlier than 4.0 maintain a database called a *bindery*. The bindery includes information such as server type, IPX address, hop count, the interface to the server, a timer value for table entries, and a list of clients. If an entry in a bindery reaches its configured maximum age without being refreshed (timer resets to zero), the router deletes the entry from that bindery.

Bay Networks routers implement a similar structure (a global services table) for these services. Each time an IPX router receives a SAP packet, it compares the packet's contents to the contents of its SAP services table. If the SAP services table already contains information about a specific service, the router simply refreshes the age timer for that entry. If the SAP services table does *not* contain information about the service, and a route exists to the service, the router adds a new entry to the services table and advertises the new service to all connected networks (except the one on which it was received).

Clients use SAP to request information about network services. Client information requests are nearest-service queries, which seek information on the closest service of a specified type. Every IPX server and IPX router on the internetwork learns about all other IPX servers and services through the propagation of bindery information or services table information.

By default, each SAP packet can contain up to seven Service Advertising updates. This number is configurable, but it's constrained by the Maximum Transmission Unit of the outbound interface.

Configurable SAP Timers

Configurable SAP timers are similar in function to configurable RIP timers, except that one pertains to SAP advertisements and the other to RIP advertisements. You configure the interval by specifying the value of the Update Interval parameter, and the multiplier by specifying the Age Multiplier parameter. By default, the age-out time is three times the standard 60-second RIP advertisement update interval, or 180 seconds.

Site Manager: Update Interval (sec) parameter: page A-42
Site Manager: Age Multiplier parameter: page A-42

Configuring SAP timers can reduce IPX SAP overhead and enhance bandwidth availability. You can eliminate periodic SAP advertisements by setting configurable SAP timers to zero; thus, only triggered SAP updates will be propagated.

To ensure proper RIP operation, all configurable RIP timers must be set at equal advertisement intervals on all Bay Networks router interfaces attached to common IPX network segments.

Note: While you can set configurable SAP timers on any Bay Networks router interface, do not use them on LAN interfaces, because IPX servers do not currently support configurable SAP broadcast timers. As a result, IPX servers will purge SAP entries after 180 seconds if they have not received any updates within this time interval.

SAP via Default Route

A SAP advertisement can be learned from an interface when the network number advertised in the SAP advertisement is unreachable, if a default route is accessible from that interface. This feature gives you the option of making SAP entries available if the IPX default route is reachable.

Site Manager: SAP via Default Route parameter: page A-19

Enabling SAP Listen and Supply Functions

The IPX router lets you enable the listen and supply modes for each IPX interface. When you enable the listen mode, the IPX router listens to SAP Periodic and Triggered updates from neighboring networks and conveys received SAP services information to its internal SAP services table.

When you enable the supply function, the IPX router transmits all SAP Periodic and Triggered updates to routers in neighboring networks.

When you enable both the listen and supply mode, the IPX router performs both the listen and supply mode functions described above.

Site Manager: Mode parameter: page A-41

Determining the Pace of SAP Packets

The SAP pace determines the frequency, in packets per second, at which SAP oackets are sent out in a circuit. By default, SAP sends out 18 packets per second on a circuit. If you enter a value of zero, there is no limit on the pace.

Site Manager: Pace parameter: page A-41

Adjusting the SAP Packet Size

By default the size of a SAP update packet is 480 bytes. You should leave the SAP packet size at the default level unless you have a specific reason for specifying a different size packet. If you must change the packet size, the packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

Site Manager: Packet Size parameter: page A-43

Responding to Nearest Server Requests

You can specify whether you want the router to respond to SAP *get_nearest_server* requests. If you have disabled split horizon, you may want to set the parameter to No.

Site Manager: Nearest Server Reply parameter: page A-43

Using a Multicast Address

By default, when you specify SAP on a router, a multicast address is used to send out SAP packets.

Site Manager: Use Multicast parameter: page A-43

Saving the Service Name

By default, a router will save all 48 bytes in the service name field of SAP packets. If you set this parameter value to No, a router will ignore all characters after the null character when a service field name is less than 48 bytes.

Site Manager: Save Full Name parameter: page A-44

Transmitting and Receiving SAP Updates Over the Same Interface

The IPX router, by default, transmits SAP updates received from the interface over that same interface. If you disable the Split Horizon parameter, the router will transmit SAP updates received from one interface, but will transmit them using routes on a different interface. Refer to the "Configurable Split Horizon" section on page 5-20 for more information about setting the Split Horizon parameter.

Site Manager: Split Horizon parameter: page A-44

Updating Routers About a Failed Service

By default, when a circuit goes down on a router, the router immediately propagates this status change to other routers in the internetwork. This facilitates network traffic by letting routers know immediately about new or failed routes. When you disable the Immediate SAP Update parameter, other routers learn about such changes only at the next periodic update interval.

Site Manager: Immediate Update parameter: page A-45

Using Static Services

When you statically configure NetWare services, the router learns about a NetWare service by means of the SAP information you enter using Site Manager. You can manually configure NetWare static services for each interface on a Bay Networks router.

When you configure static services on an interface, you can then use SAP filters to eliminate the SAP announcements. The static service provides an alternative to broadcast Service Advertisement Protocol (SAP) announcements across a WAN. The static service eliminates WAN traffic (and hence, the use of WAN bandwidth) associated with WAN SAP Announcements.

Alternatively, you can disable SAP entirely on an individual-interface basis or disable just the SAP immediate update messages. For network topologies that include slower-speed WAN links, reducing the amount of WAN bandwidth otherwise needed for SAP announcements can be helpful. You can also reduce traffic by setting the Update Interval parameter to zero, which indicates no periodic SAP updates and no aging of SAP information resulting from periodic updates. In this case, SAP immediate updates still propagate through the network. You can also configure the interface to disable immediate updates by disabling the Immediate Update parameter.

Site Manager: Update Interval (sec) parameter: page A-42
Site Manager: Immediate Update parameter: page A-45

A service sends an immediate update when one of the following conditions occurs:

- A service first comes up
- A service changes
- A service is no longer available

For more information about the Update Interval parameter, see “Configuring RIP and SAP Broadcast Timers” in this chapter.

Figure 5-7 shows a sample network configured to use static SAP services. If you want Client 1 to have access only to File Server 3, you configure File Server 3 in the static SAP Service table on Router 2’s interface. Then, to suppress any SAP broadcasts from Router 1 and thus reduce bandwidth use, you can either turn off the SAP supply or disable SAP.

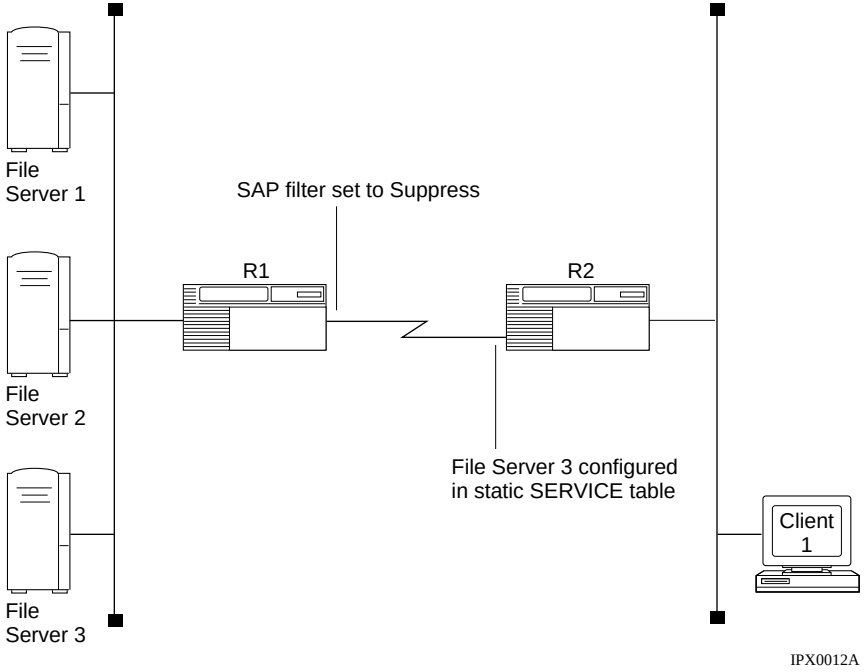

Figure 5-7. Static Service Network Configuration

Figure 5-8 shows another example, in which a SAP filter is configured on Router R1, prohibiting periodic SAP advertisements and triggered SAP updates from being propagated over the wide-area link. As a result, the services resident on Server A or Server B are not visible to Networks C and D. However, SAP services resident on Servers A and B are manually entered into Router R2's service table. This way, these servers are visible to IPX endstations on Networks C and D (through periodic SAP advertisements, which are broadcast over Router R2's LAN interfaces every 60 seconds, in conformance with IPX specifications). The key benefit in this example is that SAP overhead is eliminated over the WAN link.

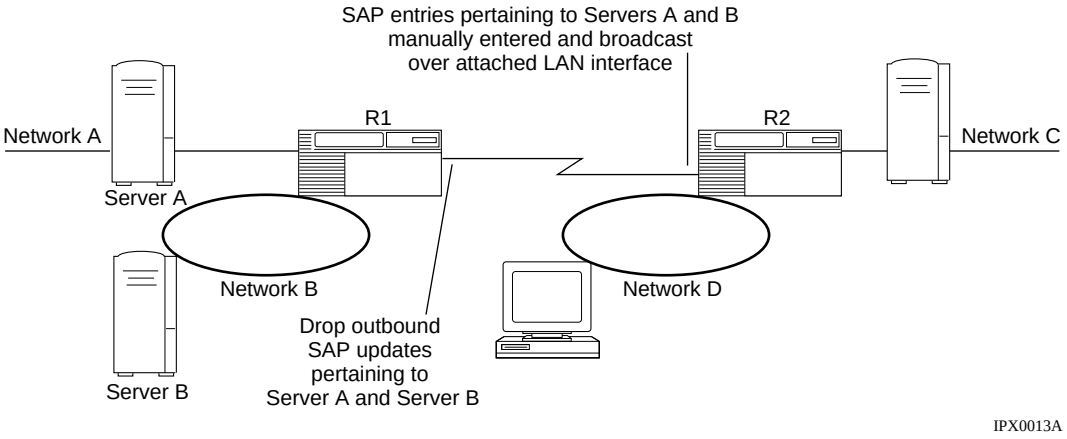

Figure 5-8. IPX SAP Filters Prohibiting SAP Broadcasts

You add, edit, or delete static services through the IPX Static Services window. For instructions, see "IPX Static Service Configuration Parameters" in Appendix A. You can configure only services that have valid network addresses. Valid network addresses are provided either by RIP or by statically configured routes. If you try to enter any services that have invalid network addresses in the router configuration, the router accepts the information, but the services are unreachable.

Note: Broadcast mechanisms, such as periodic RIP and SAP advertisements, can force dial-on-demand connections to be continuously established, preventing user-defined dial-on-demand expiration time limits from being reached. See the next section for more information.

Enabling Static Services

Enable a static service to restore client access to NetWare services configured earlier on the IPX interface. Disable a static service to make NetWare services configured earlier unavailable to clients.

Site Manager: Enable parameter: page A-62

Specifying the Network Address of a Service

When you are using a static service, the network address for the service must exist as an entry in the IPX routing table. The router can learn the entry dynamically, or you can configure the entry as a static route.

Site Manager: Target Network (hex) parameter: page A-62

Specifying the Address of the Host that Provides a Service

You must specify the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Site Manager: Host Number (hex) parameter: page A-62

Assigning a Symbolic Name to Your Service

You must assign a symbolic name to the service you want to advertise. Use the actual name of the server that the clients will attach to. Make this name meaningful to the network administrator. The name must be unique among all names assigned to IPX servers of the same type on the IPX internetwork.

Site Manager: Service Name parameter: page A-58

Entering the Service Type Number

You must specify the Novell service type number in 4-digit hexadecimal format, including leading zeros. This number specifies the type of service to advertise from the associated IPX (LAN) interface. See Appendix C for a list of common service types.

Site Manager: Service Type (hex) parameter: page A-59

Entering the Socket Address of a Service

You must enter a socket address when you are using a static service.

Site Manager: Socket (hex) parameter: page A-63

Entering the Hop Count

Enter the number of router hops that exist between a router and a specific remote Novell server or service.

Site Manager: Hop Count parameter: page A-63

Customizing NetBIOS Static Routing

NetBIOS establishes sessions (logical connections) and allows for communication between PCs. The Bay Networks NetBIOS static route function lets you map NetBIOS names to IPX destination networks by configuring a NetBIOS static route to a NetBIOS service name. The IPX router then converts the broadcast NetBIOS packets to directed broadcast NetBIOS packets, which are usually forwarded to all network interfaces on a single network. This reduces the amount of network traffic due to NetBIOS query requests; that is, broadcasts issued by NetBIOS clients seeking to find and establish sessions with specific NetBIOS applications over an IPX internetwork.

Besides minimizing NetBIOS broadcast traffic, using NetBIOS static routes allows a more precise logical partitioning of an IPX NetBIOS internetwork, enhancing internetwork security.

The Bay Networks IPX router software lets you specify whether:

- You want to direct a NetBIOS broadcast (Type 20) packet through a network by configuring a static route only at the first router. Before the packet is directed out an interface, the router software overwrites the IPX destination address of the packet so that it can be routed to its destination. Because the IPX specification states that the network address of broadcast packets must be left unchanged, this option does not conform to Novell standards.
- You want the router to propagate a packet out all of its interfaces (in conformance with Novell standards).

- You want to direct a packet to its destination by configuring a static route for each hop in the network (in conformance with Novell standards).

In the NetWare environment, NetBIOS query requests are encapsulated within IPX packets. When a Bay Networks router receives an IPX packet containing a NetBIOS query request, it compares the NetBIOS name for which a connection is being requested to a statically configured NetBIOS Name-to-IPX Destination Network table. If the requested NetBIOS name matches a table entry, the Bay Networks router forwards the query request packet out only one IPX interface toward the destination network. If a match does not exist, the router propagates the query request packet out of all IPX interfaces, in conformance with the IPX specification.

In Figure 5-9, for example, when End System ES2 wants to find and establish a connection to a NetBIOS application on the IPX Server ES2, it generates a query request broadcast packet. Router R1 receives the broadcast packet, consults its NetBIOS Name-to-IPX Destination Network table, finds that the NetBIOS application being requested is mapped to Network B, and routes the packet out Interface 1. Similarly, Router R3 consults its NetBIOS Name-to-IPX Destination Network table upon receiving the NetBIOS query request, and routes the packet out its interface to Network B.

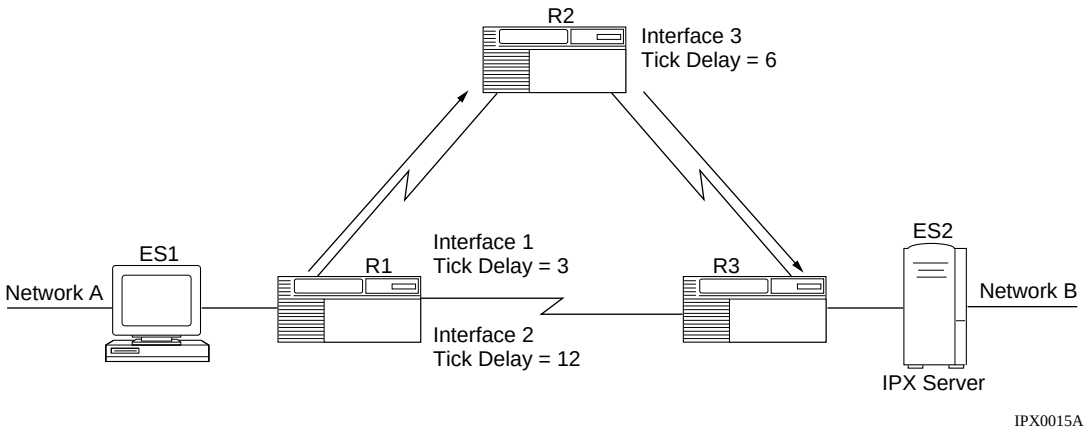

Figure 5-9. NetBIOS Static Routes

Each IPX router interface supports up to 50 NetBIOS static routes. Each NetBIOS static route specifies a NetBIOS resource name and a destination network where the resource resides.

Activating the Static Route Record in the NetBIOS Routing Table

You can specify the state (active or inactive) of the static route record in the NETBIOS routing table. If you are sending NetBIOS packets through a network, you should enable this feature.

Site Manager: Enable parameter: page A-48

Entering the Name of the NetBIOS Target Server

When you send NetBIOS packet over a network, you must specify the name of the NetBIOS target server. The name can be up to 16 alphanumeric characters. For a list of the wildcards and pattern-matching characters, refer to Table 5-1 on page 5-59.

Site Manager: Target Server parameter: page A-46

Note: The Configuration Manager does not let you reconfigure the Target Server parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route. However, you can reconfigure all other parameters associated with a static route.

Entering the Target Network Address

When you send NETBIOS packets over a network, you must specify the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.

Site Manager: Target Network (hex) parameter: page A-46

Directing a NetBIOS Packet Using Nonstandard Static Routing

You can direct a NetBIOS packet through a network by configuring a NetBIOS static route in the first Bay Networks router to receive a NetBIOS broadcast packet. To do this, you must set the Novell Certification Conformance parameter to Disabled for all routers in the network.

To configure a router to propagate a packet out all of its interfaces — which conforms to Novell standards — you set the Novell Certification Conformance parameter on the Edit IPX Advanced Global Parameters window to Enable. You must set this parameter to Enable for all routers on the network.

Site Manager: Novell Certification Conformance parameter: page A-20

All NetBIOS packets sent from a client to the router must have a destination network value of zero, unless the packet passes a static route in the router. The router tests a packet against the static route table before it checks the packet's destination, thus allowing the router to accept packets that may not have a destination network of zero.

Caution: This method of defining IPX NetBIOS static routes is a nonstandard Bay Networks feature that may not be compatible with routers from other vendors.

This method converts a NetBIOS broadcast packet to a NetBIOS directed broadcast packet, thereby eliminating the loop checking and path tracing that is usually done for NetBIOS broadcast packets. This may cause problems with applications that rely on those mechanisms.

When you configure a NetBIOS static route, the IPX router inserts the network number configured in the static route into the destination network number of the IPX packet.

When you configure NetBIOS static routes on an interface, the IPX router compares all IPX NetBIOS broadcast packets received on the interface with the boxwide NetBIOS static routes. If the NetBIOS destination name found in the packet matches an entry in the routing table, the NetBIOS packet is routed to the associated destination network. If no match is found, the IPX router treats the packet as specified by the NetBIOS Accept and NetBIOS Deliver parameters.

Directing a NetBIOS Packet Using Standard Static Routing

If you want to configure NetBIOS static routes in conformance to Novell standards, you must configure a static route for each hop in the network. After you specify the static route to a NetBIOS name, the IPX router converts standard NetBIOS broadcast packets to NetBIOS *directed* broadcast packets.

- NetBIOS broadcast packets are sent to all accessible host IDs on *all* accessible IPX networks.
- NetBIOS directed broadcast packets are sent to all host IDs on a *single* IPX network.

NetBIOS Broadcast Filters

You can control the propagation of IPX NetBIOS broadcasts by configuring NetBIOS broadcast filters on an interface. This feature ensures that visibility to NetBIOS resources is limited only to networks that need to have access to certain resources. You can configure an interface to either accept or not accept NetBIOS broadcasts from an attached network, and to deliver or not deliver NetBIOS broadcasts to a network. This capability can enhance security and preserve bandwidth by controlling the flow of NetBIOS traffic.

The NetBIOS Accept and NetBIOS Deliver parameters on the IPX Interfaces window let you configure each interface to accept and forward NetBIOS broadcasts. By default, both of these parameters are disabled.

Site Manager: NetBIOS Accept parameter: page A-26
Site Manager: NetBIOS Deliver parameter: page A-26

Note: The description that follows assumes that the NetBIOS destination name found in the packet does not match an entry in the NetBIOS Static Routing table.

With NetBIOS Accept enabled on an interface, the IPX router accepts NetBIOS broadcast packets received on that interface. For example, in Figure 5-10, the IPX router accepts NetBIOS broadcast packets received only on Interfaces 1 and 2, because the Accept parameter for those interfaces is set to Enabled.

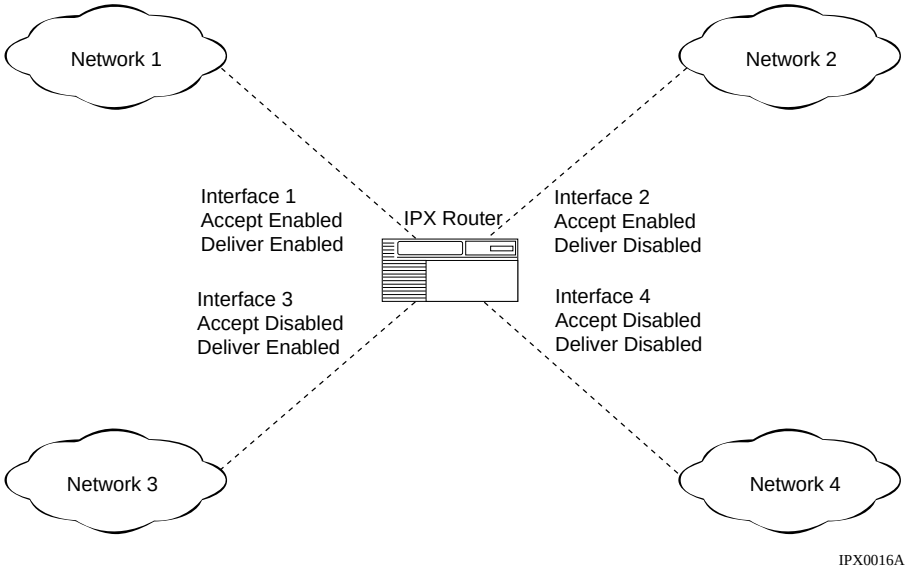

Figure 5-10. NetBIOS Packet Filtering

With Deliver enabled on an interface, the IPX router delivers NetBIOS broadcast packets that are routed to that interface. For example, in Figure 5-10, the IPX router delivers NetBIOS broadcast packets only to Interfaces 1 and 3, because the Deliver parameter for those interfaces is set to Enabled (and it's set to Disabled for the other interfaces). The arrows in Figure 5-11 show the flow of packets in this same model.

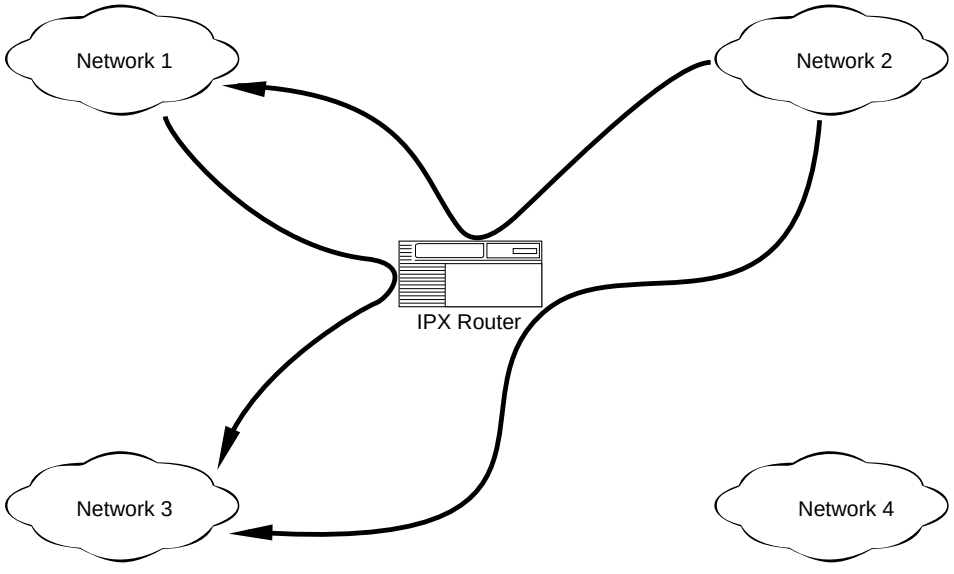

Figure 5-11. NetBIOS Packet Flow

The Accept parameter of the interface receiving NetBIOS broadcast packets and the Deliver parameter of the other interface must both be set to Enabled for delivery of such packets to occur. For example, Interface 1 can deliver only packets from Interface 2 to Network 1, because Interface 2 is the only other interface whose Accept parameter is set to Enabled.

Thus, NetBIOS client applications on Network 1 can initiate and establish sessions with NetBIOS server applications only on Network 3. NetBIOS client applications on Network 2 can initiate and establish sessions with NetBIOS server applications only on Networks 1 and 3. Client applications on Networks 3 and 4 cannot initiate any sessions with NetBIOS server applications via the IPX router.

As another example, in Figure 5-12, NetBIOS broadcasts from the End System ES1 on Network A are *accepted* by Router R1, but can be prohibited from Network C by setting the Deliver parameter on the interface of Router R1 connected to Network C to Disable. NetBIOS broadcasts will still be delivered on Network B.

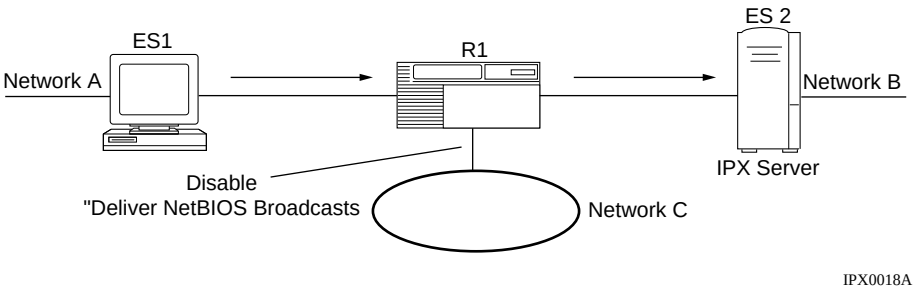

Figure 5-12. NetBIOS Broadcast Filtering

Configuring an Adjacent Host for an Interface

You can configure the adjacent host parameters if you are not using RIP on a circuit. These parameters tell the IPX router how to send a packet to a specific IPX host.

Making the Adjacent Host Record Active

Sets the state (active or inactive) of the adjacent host record in the IPX routing tables. Select Disable to make the adjacent host record inactive in the IPX host table. Select Enable to make the adjacent host record active in the IPX host table.

Site Manager: Enable parameter: page A-51

Entering the ID of the Adjacent Host

If you are not using RIP on a circuit, enter the host ID of the adjacent host. Set this parameter is you are using Frane Relay, SMDS, or ATM.

Site Manager: Host Number (hex) parameter: page A-50

Entering a WAN Address or a DLCI

If the interface you are configuring is on an ATM or SMDS network, enter a WAN address of up to 16 hexadecimal characters. If the interface is on a Frame Relay network, enter a WAN address or a decimal Data Link Connection Identifier number.

Site Manager: Host WAN Address (hex)/DLCI (decimal) parameter: page A-50

Dial Services

A dial service provides access to a switched network by means of a dial-up line (also called a *switched line*). Dial-up lines are active only as-needed -- that is, when there is data to send across the network, or when a dial-up line acts as a resource for a failed or congested leased line. Dial-up lines can be a cost-effective alternative to leased lines and packet networks, which are permanent connections and therefore available regardless of network traffic.

If you send a limited amount of data or your data transmission is intermittent, dial-up lines can be less expensive than leased lines and they maximize network performance and flexibility.

The Bay Networks router provides three types of dial services: dial-on-demand, dial backup, and bandwidth-on-demand. Each dial service serves a different purpose:

- **Dial-on-demand** service reduces your line costs by establishing a connection between two devices only when there is data to send. You do not incur the cost of a leased line that is active regardless of data traffic.
- **Dial backup** service provides a backup circuit when a leased circuit fails. The backup circuit serves as an alternative path for data to reach the destination.

- **Bandwidth-on-demand** service provides up to 29 additional lines for a congested leased line, a dial-on-demand line, or a leased multilink bundle. This provides a total of 30 lines for communication. The additional lines increase bandwidth for data traffic, improving communication and reducing network delays.

For more information about dial services, refer to *Configuring Dial Services*.

Using Dial-on-Demand Service

Dial-on-demand supports synchronous lines (RS232, V.35, RS422, and X.21) and ISDN interfaces. When dial-on-demand is configured, the router activates a dial-on-demand circuit for any one of the following reasons:

- The router has data to send across the circuit.

  When the router has data to transmit, it automatically selects one of the demand lines from the circuit's associated demand pool. As long as data is going across the line, the end-to-end connection remains active.

- You enabled a force dial. The router forces the establishment of a circuit.

  You enabled the Force Dial parameter to immediately activate a line and establish a connection. Using this parameter, you can force the connection to come up, regardless of whether there is data activity.

The router brings down the circuit for any one of these reasons:

- The configured inactivity time expires.
- You scheduled the circuit to come down.
- You enabled a forced take down.

Figure 5-13 shows a dial-on-demand line connecting two routers. In this example, when the router has data to transmit across a demand circuit, or when you configure the router to bring up a demand circuit, the router instructs the dial device to establish a connection.

Note: Don't configure IPX adjacent hosts with dial-on-demand circuits.

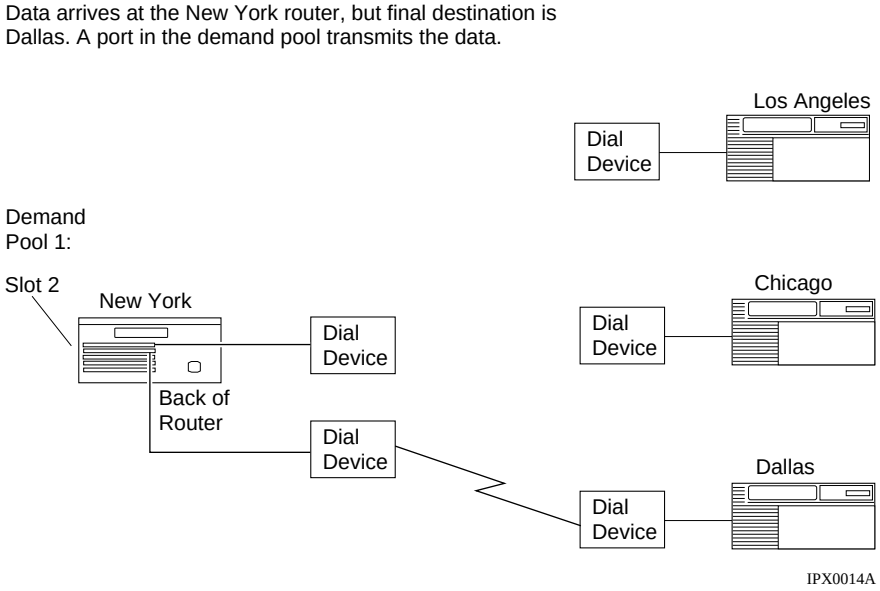

Figure 5-13. Dial-on-Demand Service

Using Static Routing with Dial-on-Demand

As part of its standard operation, IPX sends update packets to maintain routing tables and to gather information about network resources. For dial-on-demand, the frequency of these update packets forces the dial-up connection to remain up permanently, unless you configure a time of day to bring the connection down.

When you configure dial-on-demand circuits, you should disable broadcast messages. The router then uses static routes to determine the location of the destination network.

Tips for Using Dial-on-Demand with IPX

The following suggestions may help improve overall system efficiency if you're using dial-on-demand with IPX:

- Turn off triggered updates.
- Set the periodic update interval to a large value -- the line will be called only infrequently.
- Use service filtering and/or route filtering.
- Use static routes and static services.
- Use the default route.
- Enable local watchdog acknowledgment ("spoofing").
- Use traffic filters and protocol prioritization to prohibit routing updates and protocol-specific messages from keeping the circuit up unnecessarily (see *Configuring Traffic Filters and Protocol Prioritization* for details).

Local IPX Watchdog Acknowledgment

In a NetWare network, NetWare servers broadcast "watchdog" packets to verify that client nodes are still connected to the server. Watchdog packets are just another form of a data packet.

To maintain the connection, the client must respond to this watchdog message (essentially, responding to a poll). With a dial-up connection (that is, when you want to establish periodic connectivity to a remote site using the dial-on-demand feature), this polling mechanism could mean dialing the phone line just to keep the server from bringing down the connection.

In addition, the bandwidth consumed by periodic RIP/SAP and watchdog broadcast packets can represent a significant portion of the total dial cost when charged on a per-packet basis. Depending on the network configuration and the application, this excessive broadcast activity can reduce application access performance.

To address this problem, Bay Networks routers can use local watchdog acknowledgment to improve the efficiency of IPX wide-area links. This feature, also known as "watchdog spoofing," lets Bay Networks routers locally respond to broadcast IPX watchdog packets on behalf or clients connected over dial-in connections.

Site Manager: IPX Watchdog Spoofing parameter: page A-28

Without local watchdog acknowledgment, each time a server sends an IPX watchdog packet to a logically connected client, the dial-on-demand link will be established and remain up to support the communication between the client and the server (that is, the watchdog packets).

Within an IPX network, servers rely on client watchdog acknowledgments to verify that client sessions are still active with the server. The router closest to the server responds on behalf of the client. As a result, NetWare servers may reach the maximum client sessions supported by the server, although not all clients are truly maintaining a session. This can happen if the client does not perform a standard closure of the session; for example, if the client PC is rebooted. You can avoid this potential problem by implementing NetWare's auto logoff feature to ensure that client sessions are released when they are no longer in use.

Local SPX Keep-Alive Acknowledgment

In a NetWare network, SPX Keep-Alive packets are periodically transmitted to maintain SPX sessions between client and servers. To prevent these packets from initiating calls on Dial-on-Demand circuits, the router will acknowledge these SPX Keep-Alive packets.

Dial Optimized Routing

Dial optimized routing lets you exchange IPX RIP/SAP routing updates only when a connection is active for data transmission. By limiting when the router can send updates, dial optimized routing reduces unnecessary connections and line costs.

For each dial-on-demand circuit, you have the choice of enabling dial optimized routing. If you enable dial optimized routing, the router establishes a demand connection only for outbound data packets or through requests from the protocol. The presence of IPX RIP/SAP packets alone will not trigger a dial connection. If you disable optimized routing, any packet can initiate demand connections.

Once you have enabled dial optimized routing on a dial on demand circuit, the only times the router sends routing updates independent of data are

- The first time an IPX interface becomes active
- Triggered updates while the circuit is active
- Scheduled updates using a broadcast timer

You can use dial optimized routing for IPX only after you have enabled it on a PPP dial-on-demand circuit. Refer to “Configuring Dial Services” for information on how to enable dial optimized routing.

Default IPX Dial Optimized Routing Filters

When IPX is enabled on a dial-optimized routing circuit, several Priority Queuing (PQ) filters are created, by default, to reduce call initiation by various IPX packets. These filters prevent IPX Watchdog packets, SPX Keep-Alive packets, and IPX Serialization packets from initiating calls or resetting the inactivity timer on IPX demand circuits.

Enabling or disabling dial optimized routing on an IPX circuit changes the default values of the Stabilization Timer Delay to 120 seconds and RIP/SAP Update Interval to 3600 seconds. If dial optimized routing is enabled after configuring IPX on a circuit, go back and set Stabilization Timer Delay to 120 seconds and RIP/SAP Update Interval to 3600 seconds. Also, if you disable dial optimized routing, go back and change the Stabilization Timer Delay and RIP/SAP Update Interval parameters to the original default value.

Site Manager: Stabilization Timer Delay (secs) parameter: page A-28
Site Manager: Update Interval (sec) parameter: page A-36
Site Manager: Update Interval (sec) parameter: page A-42

Configuring the Routing Update Delay Timer

You can use Site Manager to define the amount of time to delay the sending of RIP/SAP updates on a circuit after the circuit has been enabled. Generally, the more routes that a router is expected to handle or the more dynamic the network is, the higher the value you should set (from 0 to 60 seconds). This timer prevents the router from dialing the remote site multiple times (each time after it collects a subset of routes). If dial optimized routing

Site Manager: Stabilization Timer Delay (secs) parameter: page A-28

RIP/SAP Triggered Updates

IPX sends triggered updates whenever a routing change occurs while the dial-on-demand circuit is active. However, with dial optimized routing enabled, triggered updates will not initiate a dial-on-demand connection. The updated information will, however, be held in the routing table and forwarded the next time the circuit comes up for data transmission or for a scheduled update.

Determining the Frequency of Scheduled Updates

By default, IPX sends out scheduled updates every 60 seconds. You can use Site Manager to regulate the frequency of broadcast updates.

The value you specify for the frequency of scheduled updates allows the router to accumulate routes for the specified period of time. The higher the number you enter, the longer the time available to accumulate routes and the less frequent the transmissions. If you enter zero, the router will not send out any periodic RIP updates over the IPX interface. However, RIP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards.

Site Manager: Update Interval (sec) parameter: page A-36

You must enable IPX watchdog spoofing or the router will continually dial the circuit whenever watchdog packets are sent. When enabled, watchdog spoofing enables a router to respond locally to IPX watchdog packets on behalf of clients. Without these packets, endpoints have no way to tell if a peer has become unreachable. This parameter also enables SPX Keep-Alive Spoofing.

Site Manager: IPX Watchdog Spoofing parameter: page A-28

Configuring RIP and SAP Broadcast Timers

A Bay Networks router running IPX lets you control the frequency of RIP and SAP update packet transmissions over both local-and wide-area links. RIP and SAP transmissions provide the following benefits:

- You spend less time manually configuring changes to static services and service routes across your network.
- You reduce the cost of administering Bay Networks routers installed across your network, compared to the cost of building static routes or static services tables.
- You allow a router to respond to changes in services and routes offered on the network.
- You enable users to have more accurate, up-to-date information on services and service routes offered on the network.

However, periodic RIP and SAP transmissions mean

- Less bandwidth is available for user data. Consequently, user data transmissions take longer, thereby increasing WAN line costs.

- You sacrifice some level of manual control over services and routes made available to network users. Your particular networking environment may require a higher degree of manual control over information on services and service routes offered to users on your network.

You can adjust the frequency of RIP and SAP update packet transmissions by specifying the Update Interval parameter (in seconds) on the IPX RIP Circuit window or the IPX SAP Circuit window (respectively) for the particular circuit. The higher the number you enter, the less frequent the transmissions. If you enter zero, no periodic RIP or SAP updates are sent out the IPX interface of the router. However, RIP and SAP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards. The default interval is 60 seconds.

Site Manager: Update Interval (sec) parameter: page A-36

Eliminating periodic RIP and SAP updates provides the following benefits:

- Reduced RIP and SAP overhead on your network
- Increased bandwidth available for user data
- Reduced WAN line costs for packet transmission
- Increased manual control over network services and routes

However, not having periodic RIP and SAP transmissions means

- A slower response time of the network to changes in network services and routes
- An increase in the time and cost of administering changes to services and service routes made available through Bay networks routers on your network

RIP and SAP timer settings should be the same on both sides of the WAN. Refer to the sections “Configurable RIP Timers” and “Configurable SAP Timers” in this chapter for more detailed information.

Using Static Routes

A static route specifies a transmission path between networks.

The static route feature lets you manually define an IPX route to a destination network. Static routes specify the next hop in the transmission path a datagram must follow, based on the datagram's destination address. You configure a static route when you want to restrict the paths that packets can follow. A Bay Networks router running IPX lets you configure static routes on each logical IPX interface.

Using static routes is most valuable over wide-area links, where bandwidth is at a premium. Static route support also enhances internetwork security because it can be implemented so that traffic across specific IPX networks is restricted, protecting sensitive internetwork resources.

Static route support for IPX can do the following:

- Direct all IPX traffic not destined for this network to an adjacent host. The adjacent host may be the actual destination, or it may be the next hop to the eventual destination network. See the following section on adjacent host support for more information about adjacent hosts.
- Reduce routing traffic by disabling the RIP supply function on all or a subset of attached interfaces that are configured with static routes.
- Provide security by eliminating all dynamic routing capabilities and all RIP supply and listen activities over an IPX interface.

You should configure static routes and disable IPX RIP and SAP advertisements when implementing dial-on-demand routing over a wide-area link. IPX RIP and SAP advertisements force dial-on-demand connections to be continuously established, which prevents user-defined dial-on-demand expiration time limits from being reached. Refer to the description of the dial-on-demand feature later in this chapter for details on using this feature.

Unlike routes learned through RIP, static routes remain in the route tables until you delete them. RIP routes have priority over static-learned routes if both routes have the same cost.

If you do not have the RIP listen functions enabled, the local network will not learn about new routes on the network, route changes, or deleted routes.

Static route support lets you identify the next interface and next router in the path toward a destination network. Once you configure a static route for an interface, the router advertises that route in its usual RIP broadcasts.

For example, in Figure 5-14, to establish a static route between IPX Network A and IPX Network B, through Interface 1 on Router R1, a static route must be established from Router R1 to Router R2. The static route entry in Router R1 directs any traffic destined for Network B through Interface 1 to Router R2. In turn, the static entry in Router R2 directs any traffic destined for Network B through Interface 3 to Router R3, and thus to Network B.

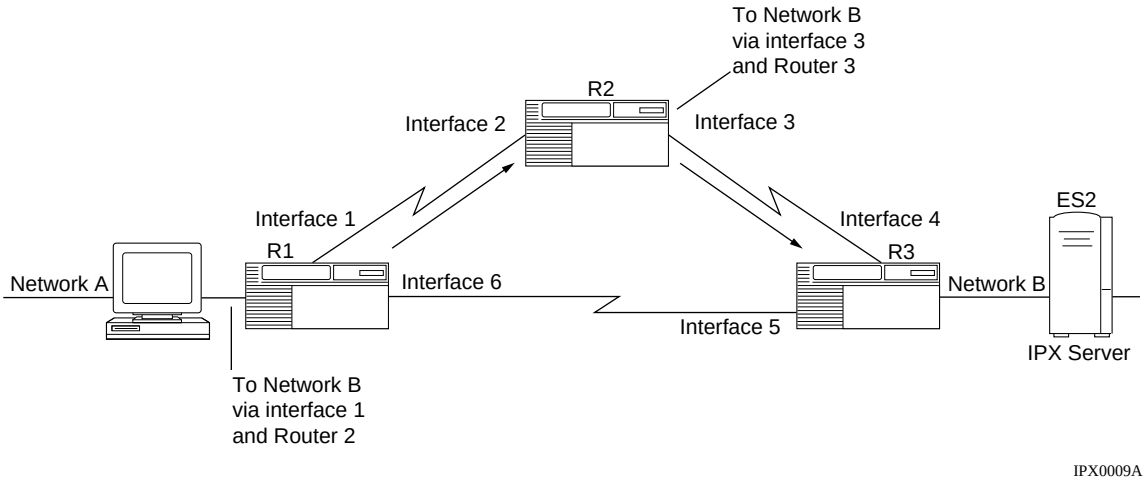

Figure 5-14. IPX Static Routes

RIP routes have priority over static-learned routes with the same cost, so if the connection between routers R1 and R3 has the same or greater cost, the packet will travel over the static route from Router R1 to Router R2 to Router R3. If a connection used by the static route fails (and if Router R1 has the listen function enabled), Router R1 will learn of an alternative route between Network A and Network B and attempt to send the packet over that connection.

IPX static routes are user-specified routing table entries. Static routes, like routes learned through RIP, are maintained in the IPX routing table. Unlike routes learned through RIP, however, static routes do not expire. Static routes remain in the IPX routing table until they are reconfigured manually. Static routes are removed if the interface they are configured on goes down.

Note: You can send packets over a static route if you have mapped an IPX host address to a data link address in a Frame Relay, SMDS, or ATM network. If RIP is disabled on a WAN interface, before you configure a static route to an adjacent host, you must configure an adjacent host and edit the DLCI parameter.

Specifying the Target Network Address

If you are using the static route feature, you must specify the address of the network to which you want to configure the static route.

Site Manager: Target Network (hex) parameter: page A-53

Entering the Next-Hop Host

With the static route feature, you must specify the address of the next-hop host in the static routing path. The next hop host is the host address of the down-stream router's IPX interface.

Site Manager: Next Hop (hex) parameter: page A-54

Entering the Hop Count

The IPX router uses Hop Count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means "use the hop count associated with the interface."

Site Manager: Hop Count parameter: page A-54

Setting the Timer Ticks

With the static route feature, you specify the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.”

Site Manager: Ticks parameter: page A-55

Using Route Filters

You can shield the view of networks from users on different network segments by configuring route filters. Route filters give you greater control over the routing of IPX packets from one area of an IPX internetwork to another. This helps maximize the use of the available bandwidth throughout the IPX internetwork, and helps improve network security by shielding a user’s view of other networks.

You can configure inbound or outbound route filters on a per-interface basis, instructing the interface to advertise/accept or drop filtered RIP packets. The action parameter that you define for the filter determines whether the router advertises, accepts, or suppresses RIP packets from routers that match the filter pattern.

IPX route filters uses the network number field in the IPX RIP packet. Network filtering is based on a two-part definition: filter ID and a corresponding mask. A route filter can be inbound, outbound, or both. You can define filters by network address, or by a range of network addresses.

The filter ID and the mask definition work together to determine which addresses are filtered on the interface. The character F in the mask definition requires an exact match with the corresponding character in the filter ID. The mask character 0 matches any hexadecimal character. You can combine the F and 0 characters in any order in the mask to filter any combination of network and/or area addressing schemes used within the IPX internetwork.

For example, suppose you want to filter the range of network addresses from ABCD1200 to ABCD12FF. To do this, you would define:

- A filter ID of ABCD12FF, *and*
- A mask of FFFFFF00

In this example, the filter ID says “This is the pattern to match.” The mask says, “The first six characters of the address must match the filter ID, but the last two characters are irrelevant.”

The IPX Route Filters window displays each route filter entry in the router configuration, as follows:

<rule_number>, <priority>, <circuit_index>, <filter_ID>, <filter_mask>

Once you have configured route filters, you can easily drop all routes to allow one or more specific routes. To drop all routes, apply a filter at a low priority. For example, in the IPX Route Filters window, enter the value 0xFFFFFFFF for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask, and set the Action parameter to Suppress.

Add the filters you want by specifying higher priorities to advertise specific routes. For example, enter the value 0x3081be86 for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask parameter, and set the Priority parameter to 1.

Using SAP Filters

Briefly, a filter is a pattern for matching a service name or service network. The router scans incoming and outgoing SAP packets to see whether certain fields in the packet match the filter. (The type of filter -- service name or service network -- determines which fields the router examines.) When you set up the filter, you can specify what the router does with the services in the packet when it finds a match.

You can create SAP filters on Bay Networks routers in your network to regulate both incoming and outgoing SAP advertisements. You can use SAP filters to control the size of resident SAP services tables and reduce bandwidth waste on your network due to SAP broadcast overhead. You can also create SAP filters as a security mechanism to limit a user’s view of services located elsewhere on the network.

Each SAP filter consists of a service name or network number, a service type, a priority, and a configurable action parameter. (You can also include wildcards or patterns to be matched). As a result, you can tailor SAP filters to your site requirements, improving network security by controlling access and preserving bandwidth by limiting the SAP packet traffic.

On a given interface, you can configure a filter as inbound, outbound, or both.

- *Inbound* filters affect only incoming SAP advertisements. The filter determines whether the Bay Networks router accepts or suppresses the service information from certain servers, based upon the action that you specify.
- *Outbound* filters affect only outgoing SAP advertisements. The router either advertises or suppresses SAP information, depending on whether it matches the filter's content, based upon the action that you specify.
- *Both* applies the same filter pattern to both incoming and outgoing SAP advertisements.

Site Manager: Mode parameter: page A-68

Figure 5-15 shows an example of SAP outbound filtering.

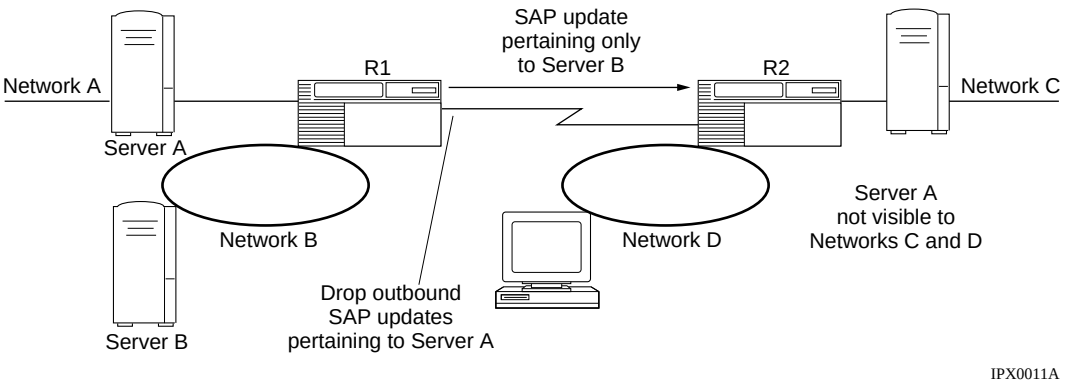

Figure 5-15. SAP Filtering

In this example, a SAP filter configured on Router R1 prevents SAP advertisements and updates pertaining to Server A from being propagated over the wide-area link. As a result, Server A is invisible to Networks C and D. Information pertaining to Server B, however, continues to be propagated over the WAN link.

Note: While SAP filters restrict a user's view of network service information, they do not prevent users from accessing services. If users have access to resources contained on an IPX network, they can also access all services within that network, regardless of whether a service has been filtered. It's like telling the Post Office to discard all sale flyers that you receive from a certain store. You assume that the store still exists, and you can still go to and buy from that store, even though you may not know its latest specials. The IPX router always updates its own SAP services table according to inbound SAP data.

You can configure SAP filters using the following levels:

- You can filter SAP service information pertaining to individual servers by editing server-level SAP filters.

  At the service level, the filter matches a pattern that you specify (consisting of a service name pattern and a service type). The filter's Action parameter determines the action (Accept/Advertise or Suppress).

Site Manager: Action parameter: page A-69

- You can filter service information pertaining to entire networks by editing network-level SAP filters.

  At the network level, the filter matches a pattern that you specify (consisting of a service network number and a service type). The filter's Action parameter determines the action (Accept/Advertise or Suppress).

Site Manager: Target Server parameter: page A-82
Site Manager: Target Service Type (hex) parameter: page A-82
Site Manager: Action parameter: page A-84

The IPX router with an outbound filter configured on an interface includes information about a service in a SAP packet if either of the following is true:

- The router finds a match between an outbound filter's contents and the service in its SAP services table, and the filter action is Advertise/Accept.
- The router does not find an outbound filter that matches the service in its SAP services table.

The IPX router excludes information about a service from a SAP packet only if it finds a match between an inbound filter's contents and the contents of its SAP services table, and the filter action is Suppress.

Similarly, the IPX router accepts information about a service in a SAP packet if either of the following is true:

- The router finds a match between an inbound filter's contents and the service in the SAP packet, and the filter action is Advertise/Accept.
- The router does not find an inbound filter that matches the service in the SAP packet.

Using Wildcards and Pattern Matching with SAP Filters

Wildcards and pattern matching are shortcut techniques for setting up SAP filters. Wildcards are characters that match zero or more instances of any valid character. In other words, a wildcard in a filter matches any allowable character(s), depending on which wildcard you specify. Pattern matching lets you selectively filter by named entities. The following sections describe each of these techniques.

Using Wildcards with SAP Filters

Wildcards in SAP filters let you configure a single SAP filter to match a set of services. When you use wildcards, you can configure the filter based on the service name, which lets you configure a SAP filter based on the characters represented in the service name field of an IPX SAP packet. The service name field contains the 48-byte character string name that is assigned to a NetWare server. The service name, in combination with the service type, uniquely identifies a service on the internetwork. You can use a wildcard SAP filter configured using the service name field to shield users' view of services that reside on a group of servers that use a common naming convention.

The wildcard characters are

* (Asterisk) matches any number of instances (zero or more) of the previous character.

• (Period or dot) matches any *single* character.

For example, suppose an organization has ten servers within its network, each providing a variety of different services. Five of the servers have names that begin with the character **p**, while the other servers have names that start with a different character. You could then define a single SAP filter **p•*** that would filter all SAP information for all five servers whose server name begins with the character **p**.

Similarly, a SAP filter defined as p•int would match the server names **print**, **point**, and **paint**, but not the server name **poing**, because the wildcard character • matches only a single character in the same position in the string that makes up the server name.

Using Pattern Matching with SAP Filters

You can also filter SAP packets by, matching a filter pattern that you define as a *regular expression*, using the characters shown in Table 5-1. The software compares this regular expression against a service name and returns an indication of whether it finds a match. Functionally, pattern matching on SAP filters is similar to the UNIX **grep** command.

Table 5-1. Characters in SAP Pattern Matching Filters

Filter Character	Function
C	Matches any character, except those listed below. An ordinary character (like a, b, 7, or q) matches only itself.
\ (Backslash)	The backslash (\) is the escape character. Use this to match a character that would otherwise have special meaning to the software. The special characters that must be preceded by a backslash to match themselves are **** (backslash) **.** (period or dot) **[** (left bracket) **?** (question mark) ***** (asterisk) **{** (left brace) **(** (left parenthesis) **)** (right parenthesis) **|** (vertical bar) **$** (currency symbol) Must be quoted only when it's the last character to be matched. Any other quoted character following a backslash matches itself. For example, to match a backslash (\) in a string, include the following in the filter expression: \\
. (Dot or period)	Matches a single character Example: **SERVER.** Matches: SERVER1 and SERVERA Does not match: SERVER12 or SERVER
[c...]	As the rightmost element in a string, this element tells the filter to match *any one* of the characters enclosed in the brackets. To use a right bracket (]) as one of the characters to be matched, make it the first character in the string. The expression: [ ]abc] matches any of the characters:], a, b, or c

Table 5-1. Characters in SAP Pattern Matching Filters *(continued)*

Filter Character	Function
[^c...]	When a caret is the first character of the enclosed string, the filter expression matches any character *except* those in the remainder of the string. For example, the expression [^45678] matches any character except 4, 5, 6, 7, or 8. To include a right bracket (]) in the string of filtered characters, place it directly after the caret. For example, the expression [^] abc] matches every character except], a, b, or c.
[l-r]	The minus sign between two characters indicates a range of consecutive ASCII characters to match. This bracketed string of characters is known as a *character class*. For example, the range: [0-9] is equivalent to the string: [0123456789] The minus sign (-) is treated as an ordinary character if it occurs first (or first after an initial ^ character) or last in a string.

You can also construct longer filters by combining (that is, concatenating) these single-character regular expressions using the rules and operators listed in Table 5-2. A filter made up of a concatenation of regular expressions matches a concatenation of text strings, each of which is a match for a successive regular expression in the search pattern.

Table 5-2. Concatenation Rules and Operators

Rule/Operator	Interpretation
? (Question Mark)	A single-character regular expression followed by a question mark (?) matches *zero or exactly one* occurrence of that single-character regular expression. For example, [a-z]**?** matches any string of either zero lowercase letters or exactly one lowercase letter. Example: **SERVER?** Matches: SERVER1 and SERVER Does not match: SERVER12 or SERVER123
***** (Asterisk)	A single character regular expression followed by an asterisk (*) matches zero or more occurrences of that single-character regular expression. For example, [a-z]***** matches any string of zero or more lowercase letters. Example: **SERVER*** Matches: SERVER123 and SERVER Does not match: ADMIN123 or PS_SERVER
+ (Plus Sign)	A single-character regular expression followed by a plus sign (+) matches one or more occurrences of that single-character regular expression. For example, [a-z]+ matches any string with one or more lowercase letters. Example: **SERVER+** Matches: SERVER12 and SERVERA Does not match: SERVER or ADMIN123
{m} **{m,}** **{m,n}** (Where m and n are integers)	A one-character regular expression followed by {m}, {m,}, or {m,n} is a regular expression that matches a range of occurrences of the one-character regular expression. The values m and n must be non-negative integers less than 255. The symbols in braces mean the following: {m} matches *exactly* m occurrences {m,} matches *at least* m occurrences {m,n} matches *any number* of occurrences between m and n. Whenever a choice exists, the regular expression matches as many occurrences as possible. For example, the **?** operator is equivalent to {0,1}, the ***** operator is equivalent to {0,}, and the **+** operator is equivalent to {1,}.
Use the following operators to construct regular expressions from more-than-single-character regular expressions.	

Table 5-2. Concatenation Rules and Operators *(continued)*

Rule/Operator	Interpretation
(...) (Regular expression(s) enclosed in parentheses)	A regular expression enclosed within parentheses matches whatever the unadorned regular expression matches. You use parentheses to group a series of regular expressions that you want to have treated as a single-character regular expression. For example, the regular expression **0[Xx]?** matches a 0 that may or may not be followed by one X or x, while the regular expression **(0[Xx])?** matches either nothing or the string "0X" or the string "0x". You can have up to nine such substrings in a regular expression, and you can nest parentheses.
| (Vertical Bar)	Two regular expressions separated by the vertical bar (|) match either a match for the first or a match for the second. These two regular expressions are the longest that can be created subject to parentheses grouping. For example, these regular expressions are grouped as follows: and|or = and | or and*|o+r = and* | o+r a(nd|o)r = a, plus either nd or o, plus r Example: **SERVER(8FS|1FS)** Matches: SERVER8FS and SERVER1FS Does not match: SERVER or SERVER5FS
[ ] (Square Brackets)	Matches any single character in the bracketed set.. Example: **SERVER[123]** Matches: SERVER1 and SERVER3 Does not match: SERVER123 or SERVER23

The server name filters take precedence over the service network filters. Both service name and service network filters have an associated priority, with smaller values denoting a higher priority. Matching is performed by first checking all service name filters in order by priority. If a match isn't found, then the service network filters are checked in order by priority.

For example, you may want to advertise from an IPX interface only one type of service (Type 4) belonging to a particular server (Server 1). You can configure:

- A service name SAP filter with a target service name of Server 1, a service type of 4, and an action to advertise.

- A service network filter with a target network of 0xFFFFFFFF, a type of 0xFFFF, and an action to suppress. (This service network filter prevents all other services from being advertised from the interface.)

Using similar specifications and an action to suppress, you could exclude from an IPX interface a type of service from a particular server.

Note: The order in which you create SAP filters does not affect filter precedence.

An Example of Using SAP Filters

The following example describes a situation in which you might want to configure SAP filters. An office complex contains three buildings. The people in each building use only the print services within their own building and have no need to send files to printers outside their building. To free wasted bandwidth, you could configure a SAP filter that suppresses print server advertisements on the interfaces of the routers that connect the three buildings.

To suppress print server advertisements, configure a service network filter on the interfaces of the routers that connect the three buildings and suppress the advertisement of Server Type 0x0047 (print server) for all networks (0xFFFFFFFF). Refer to Appendix A for a list of common server types.

The IPX Service Network window displays each service network filter entry in the router configuration, as follows:

<filter/rule_no.>, <filter_priority>, <circuit_number>, <target_network_number>, <target_network_mask>, <target_service_type>

Once you have configured SAP filters, you can easily drop all services to allow one or more specific services. To drop all services, apply a filter at a low priority.

Example

In the IPX Service Network Filters window, enter the value 0xFFFFFFFF for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask, and set the Action parameter to Suppress.

Site Manager: Target Network (hex) parameter: page A-67
Site Manager: Target Network Mask (hex) parameter: page A-67
Site Manager: Action parameter: page A-69

Add the filters you want by specifying higher priorities to advertise specific services.

Example

Enter the value 0x3081be86 for the Target Network parameter, the value 0xFFFFFFFF for the Target Network Mask parameter, the value 0x0004 for the Target Service Type parameter, and set the Priority parameter to 1.

Site Manager: Target Network (hex) parameter: page A-71
Site Manager: Target Network Mask (hex) parameter: page A-72
Site Manager: Target Service Type (hex) parameter: page A-72
Site Manager: Filter Priority parameter: page A-73

Editing Service Name Filter Parameters

The service name filters function lets you reduce network traffic by configuring service name filters.

The IPX Service Name Filters window displays each service name filter entry in the router configuration as follows:

<filter/rule_no.>, <filter_priority>, <circuit_index>, <target_service_name>, <target_service_type>

Enabling an IPX Service Name Filter

If you are configuring service name filters, you must activate this feature for each interface.

Site Manager: Enable parameter: page A-81

Entering the Target Service Name

Enter a service name or filter pattern that you want to apply.

Site Manager: Target Service Type (hex) parameter: page A-82

Entering the Target Service Type

If you are using a service name filter, you must specify the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment. See Appendix C for a list of common service types.

Site Manager: Target Service Type (hex) parameter: page A-82

Setting the Filter Priority

Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities.

Site Manager: Filter Priority parameter: page A-83

Applying Filters to Inbound or Outbound Packets

You can apply the service name filter to inbound packets, outbound packets, or both. By default, the filter is applied to SAP packets advertised by the specified interface. If you want to apply the filter to SAP packets coming into this interface, specify inbound. If you want to filter both incoming and outgoing packets, specify both.

Site Manager: Mode parameter: page A-83

Specifying the Protocol

When you send SAP updates, you can apply this outbound filter only to services learned on the specified protocol. This feature does not apply to inbound services.

Site Manager: Protocol parameter: page A-83

Specifying How to Process SAP Advertisements

You can specify how the router should process any SAP advertisement that matches the SAP filter criteria you established in the Target Service Name and Target Service Type parameters.

Select Advertise/Accept to enable the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Service Name and Service Type parameters.

Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Service Name and Service Type parameters.

Site Manager: Action parameter: page A-84

Specifying a Cost

If you are enabling the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Service Name and Service Type parameters, you can assign a cost (number of ticks or hops) for this interface.

Site Manager: Cost parameter: page A-85

Source Route Bridge Endstation Support

Source route bridge endstation support enables routable traffic generated in a source route bridge environment to be routed to workstations on remote LANs over a multiprotocol backbone. The Bay Networks router running IPX lets you configure source route endstation support for Token Ring networks on each interface. This allows bridging and routing to coexist in the same IBM source route bridging environment. With endstation support enabled, endstations that support both source route bridging and IPX can use source routing to traverse bridged networks.

In a source routing network, every endstation supplies each frame it sends out with route descriptors, so that it can be source routed across the network. Thus, for routers running IPX to route packets across a source routing network, they must act like endstations, supplying route descriptors within each packet before sending it onto the network.

All traffic is source route bridged within the local Token Ring environment. Routable traffic intended for a destination on a LAN interconnected through a multiprotocol backbone is routed over the backbone by the Bay Networks node. With endstation support enabled, the Bay networks router running IPX does the following whenever it receives a packet and determines that the packet's next hop is across a source routing network:

- Sends out a Single Route Explorer (SRE) frame to discover a path to the next-hop network.
- Adds the necessary Routing Information Field (RIF) information to the packet's MAC header.
- Sends the packet to the network, where it is source routed toward the next hop.

After the peer router receives the packet from the Token Ring network, it strips off the RIF field and continues to route the packet toward the destination network address, as shown in Figure 5-16.

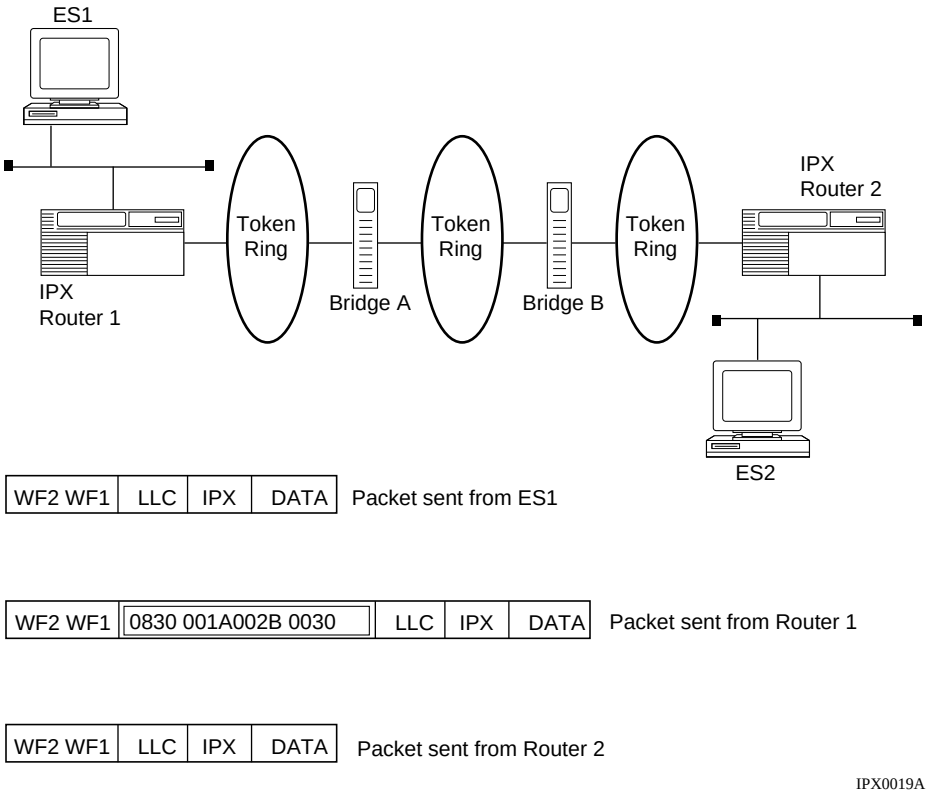

Figure 5-16. IPX Routers Source Routing Across a Token Ring Network

You configure source route endstation support on each interface by setting the TR End Station parameter to Enable.

Site Manager: TR End Station parameter: page A-25

The transition to network-layer routing outside the source route bridge environment can improve overall network performance by reducing source route bridge overhead on a WAN and can maximize network availability by rapidly rerouting around a failed link.

IPX Ping Support

The Bay Networks Site Manager supports the IPX ping feature, which uses an IPX diagnostic packet to ping NetWare servers to determine the accessibility -- that is, the status, “alive” or “not responding” -- of the following:

- A remote Bay Networks router
- A Novell IPX server (except as noted below)
- A Novell multiprotocol router
- A NetWare client

This feature can be particularly useful in troubleshooting large networks.

Note: In conformance with the Novell specification, a Bay Networks router running IPX will respond to pings from NetWare servers but will not initiate pings to those servers. Instead, the router running IPX will use diagnostic packets to accomplish the ping function.

Using the IPX ping command, the router attempts to communicate with another router running IPX, a server, or an IPX client, and determines whether the destination node is functioning and reachable from the source node. The “pinging” Bay Networks router sends an IPX diagnostic packet, called a *Configuration Request*, and either the “pinged” router running IPX, the server, or the IPX client responds with a *Configure Response* packet.

See *Managing Routers and BNX Platforms* for instructions on using the ping feature in IPX.

Role of Bay Networks Routers in a Client/Server Connection

This section describes how Bay Networks routers running IPX provide clients access to servers on an IPX internetwork.

- Router builds SAP and RIP tables

  The Bay networks router builds its routing and services tables by listening to regularly scheduled SAP and RIP broadcasts from file servers. The broadcasts include the services a server has to offer and routes to a server. If regular SAP or RIP broadcasts from a file server stops, the local router ages out the entry and removes it from its services or route table.

- Client sends *get_nearest_service/get_nearest_directory_server* SAP request

  A client sends this request to locate a file server. (Refer to the book, *Novell's Guide to NetWare LAN Analysis*, by Laura Chappell and Dan E. Hawkes, for more information on this mechanism.)

- Router decisions

  If the server resides on the same network as the client, the server receives the request and responds. The local router does not respond because its services table indicates that the service is available on the client's network. In this case, client-router communications stop until the client sends the next *get_nearest_service* SAP request.

  If the server does not reside on the same network, the router responds, because its services table indicates that the service is not available on the client's network. The SAP response sent by the router contains the server name, the internal address (if applicable), the service type, the socket number, and the intervening network count of the nearest device offering the service. Continue to the next bullet.

  If the server does not reside on the same network and multiple servers of the same service type are available, the router picks the server that is the fewest ticks away. If two servers are the same number of ticks away, then the router chooses the server that is the lowest number of hops away. If two servers are the same number of ticks and hops away, then the router chooses based on the alphanumeric order of the server names listed in the services table.

- Client's RIP request

  The client then broadcasts a RIP request packet to the local segment. This packet requests the best path to the server's network.

- Router's RIP response

  The router on the same network as the client refers to its route table and sends a RIP response to the client. The RIP response identifies the network on which the client resides. The RIP response also contains the server's internal network address and the intervening hop and tick count.

- Client's NCP Request

  The client sends a Network Core Protocol (NCP) create connection request to the server. The request includes the router's MAC address as the destination address at the data link layer. Within the IPX header, the destination network address is the internal address and the destination node address of the file server. The client forwards the packet to the router.

- Router forwards packet

  The router running IPX forwards the packet to the network identified by the destination network address.

Example: Client/Server Connection via Bay Networks Router

In the example shown in Figure 5-17, Client A sends a SAP request to locate a file server. Here's what happens as a result of that request.

1. Because the server does not reside on LAN A (the same LAN as Client A), the Bay Networks IPX router, Host 2, sends a SAP response to Client A, informing it that the File Server, Host 3 on Token Ring 6, is the nearest device offering the requested service.
2. Client A then sends a RIP request to determine the best path to Host 3.
3. The Bay Networks IPX router, Host 2, sends a RIP response to Client A that includes the server's internal network address and the intervening hop and tick count from Host 3 to Client A.
4. Client A sends an NCP request packet to the Bay Networks IPX router, Host 2.
5. The router then forwards the packet to Host 3.

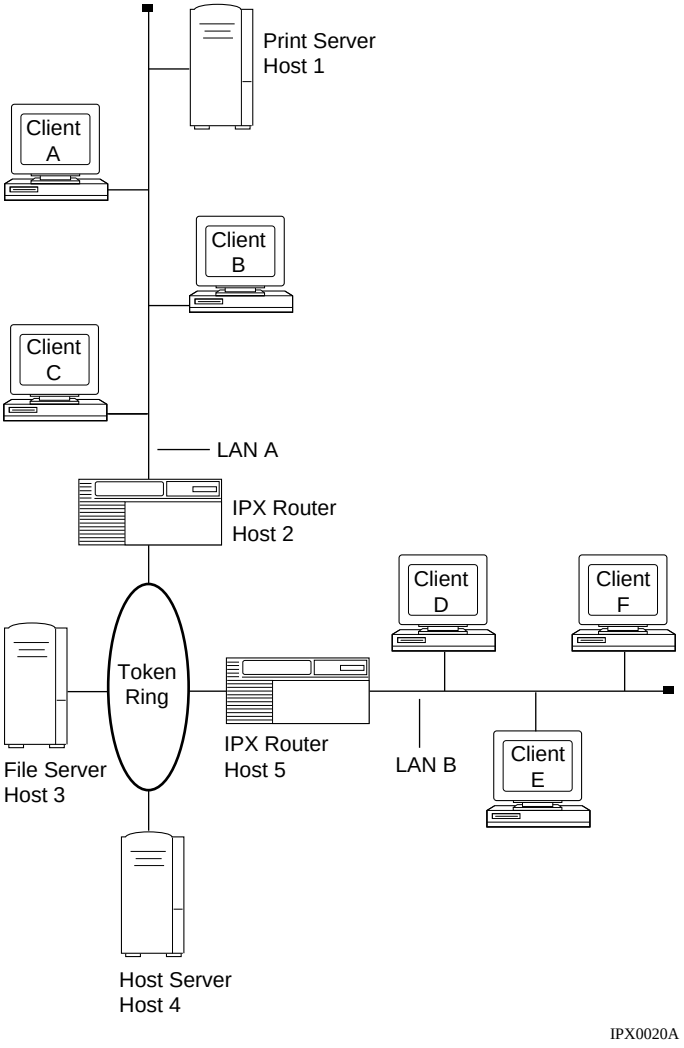

Figure 5-17. Sample IPX Network

Appendix A
IPX Parameters

This appendix explains all the IPX parameters and how to use them if you want to customize an interface you have added to a router.

IPX Configuration Parameters

The IPX configuration parameters enable you to get IPX up and running quickly by supplying only the necessary configuration information and accepting the defaults supplied by Bay Networks for all other Site Manager parameters. You access these parameters via the IPX Configuration window (Figure A-1). This window may appear differently depending on the WAN protocol you choose in the Select WAN Protocols window.

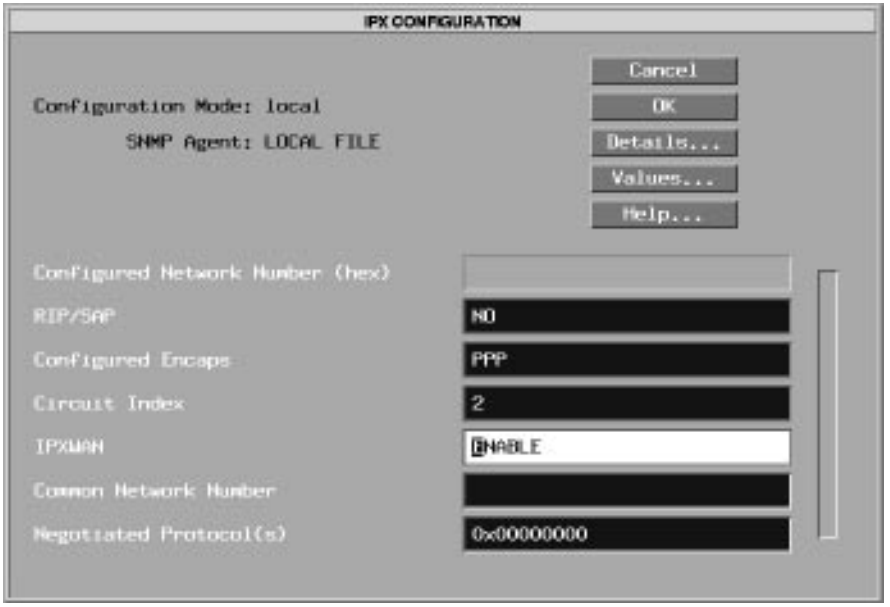

Figure A-1. IPX Configuration window

Parameter: Configured Network Number (hex)

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX network number in hexadecimal format

Function: Identifies the IPX network number that the user assigned to this IPX circuit. This parameter is active only for circuits that are not configured as IPXWAN interfaces or for those with the IPXWAN parameter explicitly disabled.

Instructions: Enter a valid IPX network number in hexadecimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.22

Note: The Configured Network Number parameter is active only for circuits that are not configured as IPXWAN interfaces. The IPXWAN, Common Network Number, and Negotiated Protocols parameters appear only when the circuit is configured as an IPXWAN interface.

Parameter: RIP/SAP

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: Depends on whether you enabled RIP/SAP in the Select Protocols window.

Options: Yes | No

Function: Indicates whether you have RIP/SAP configured on an interface.

Instructions: The Configuration Manager sets the default for this parameter based on your selection in the Select Protocols window. If you selected RIP/SAP, both RIP and SAP are enabled. You can disable both RIP and SAP using the IPX Configuration window. You can also disable and re-enable just RIP or just SAP using the RIP Circuit window or the SAP Circuit window, which are available via the IPX Interfaces window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.1 (RIP)

1.3.6.1.4.1.18.3.5.5.33.1.1 (SAP)

Parameter: Configured Encaps

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: Circuit medium dependent

Options: Circuit medium dependent (see Instructions)

Possible values: Ethernet | LSAP | Novell | SNAP | PPP

Function: Specifies the encapsulation methods (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, Token Ring, or sync). The encapsulation method supports communication on a specific logical network.

Instructions: Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows:

- Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.
- Token ring circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.
- FDDI circuits support LSAP and SNAP frames.
- HSSI circuits support PPP and SNAP frames.
- ISDN circuits support PPP frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter: Circuit Index

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: System-assigned

Options: Any valid circuit identifier

Function: Uniquely identifies this circuit within this instance of IPX.

Instructions: Accept the default or enter a valid circuit identifier.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.6

Parameter: **IPXWAN**

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPXWAN for this interface on this router. This parameter is active only for circuits that are configured as IPXWAN interfaces.

Instructions: Select Enable to turn on IPXWAN negotiation for this interface.

Select Disable to turn on IPXWAN negotiation for this interface.

MIB Object ID: Not Applicable

Parameter: **Common Network Number (hex)**

Path: Configuration Manager > Select Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX network number, 0x00000000 to 0xFFFFFFFD in hexadecimal format

Function: Specifies the IPX common network number assigned to this IPX circuit. This parameter is active only for circuits that are configured as IPXWAN interfaces that have the IPXWAN parameter enabled.

Instructions: Enter a valid IPX network number in hexadecimal format. Do not use the values 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.24

Parameter:	**Negotiated Protocol(s)**
Path:	Configuration Manager > Select Protocols > IPX > Interfaces
Default:	Unnumbered RIP
Options:	RIP | Unnumbered RIP
Function:	Indicates the protocol negotiated for this interface. This parameter is active only for circuits that are configured as IPXWAN interfaces and that have the IPXWAN parameter enabled.
Instructions:	Accept the default or click on Values to display the other choices. You can select more than one option. Click on the options you prefer, then click on OK to accept your choices. The parameter value appears as a hexadecimal number on the IPX Change Circuit window. The values are as follows: 0x00000008 RIP 0x00000010 Unnumbered RIP 0x00000018 RIP and Unnumbered RIP
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.8

IPXWAN Configuration Parameters

The IPX configuration parameters enable you to get IPX using IPXWAN services up and running quickly by supplying only the necessary configuration information and accepting the defaults supplied by Bay Networks for all other Site Manager parameters. You access these parameters via the IPXWAN Configuration window (Figure A-1). This window appears after you enable IPXWAN services in the IPX Configuration window.

Figure A-2. IPXWAN Configuration Window

Parameter: Router Name

Path: Configuration Manager > Select Protocols > IPX > Enable IPXWAN

Default: None

Options: Any valid NetWare router or server name

Function: Specifies a symbolic name for the router. Any IPXWAN (RFC1634-compliant) interface in the node uses this name to identify itself to the IPX router or server at the opposite end of the WAN data link.

The symbolic name for the router must be unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a router or server name. It's a good idea to make the name meaningful to users as well as routers

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.9

Parameter:	**Primary Net Number (hex)**
Path:	Configuration Manager > Select Protocols > IPX > Enable IPXWAN
Default:	None
Options:	The Primary Network Number (PNN) is a string of up to 8 hexadecimal characters.
Function:	Specifies an IPX network number for IPXWAN (RFC1634-compliant) link negotiation on all slots. The value of the PNN determines whether the local or remote WAN interface serves as IPX Link Master. The node with the highest PNN value becomes the IPX Link Master. The PNN should be unique among network numbers currently assigned.
Instructions:	Enter a unique network number for each node requiring one or more IPXWAN (RFC1634-compliant) interfaces. (This network number must be unique across the IPX network. Do not enter a number that a server is using as an internal network number, or a number that has been assigned on any segment in the network.) All unused values between 0x00000001 and 0xFFFFFFFD are valid values.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.5

IPX Global Parameters

The IPX global parameters determine the way IPX works on the router. You access these parameters via the Edit IPX Global Parameters window (Figure A-3).

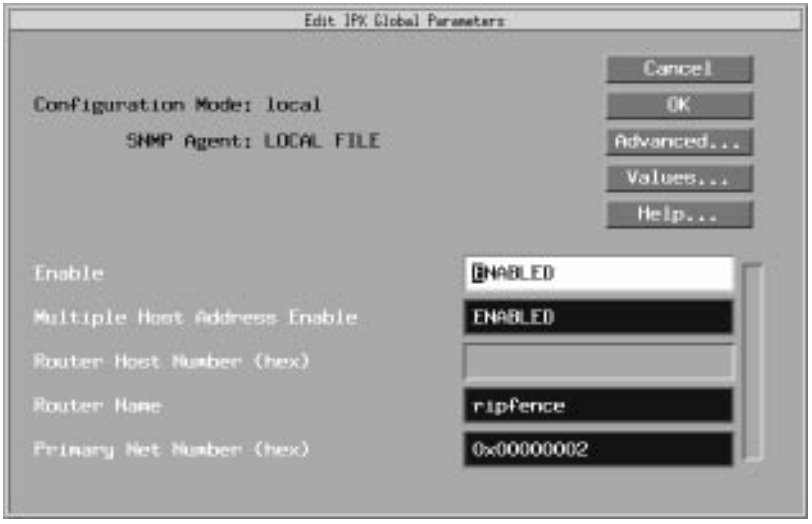

Figure A-3. Edit IPX Global Parameters window.

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Global

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the system software mechanisms that allow users to add IPX interfaces to the router configuration:

Disable -- Shuts down all IPX routing for the entire router.

Enable -- Initializes IPX routing for the entire router. Associated IPX interfaces become active, depending on their respective Enable | Disable parameters and on the state of each underlying circuit.

Instructions: Select Disable to disable every IPX interface on the router.

Select Enable to globally reinitialize all IPX interfaces on the router; each interface maintains the most recent setting of its own interface Enable | Disable parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.2

Parameter: Multiple Host Address Enable

Path: Configuration Manager > Protocols > IPX > Global

Default: Enable

Options: Enable | Disable

Function: If you enable this parameter, an IPX interface can

- Use the MAC address located in the PROM on the circuit associated with that interface
- Use a MAC address that you enter in the Host Number parameter field for that interface. Interfaces on a Token Ring circuit adopt a host ID number based only on the MAC address of the associated circuit.

Disabling this parameter causes all IPX interfaces to adopt a single host ID number for the entire host, based either on the serial number of the router backplane or on a number that you enter in the Host Number parameter field.

Instructions: Choose Enable or Disable, as appropriate for the type of configuration (standard, multiple interfaces per circuit, or multiple circuits per physical segment). See Chapter 2 for a description of each type of configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.6

Parameter: **Router Host Number (hex)**

Path: Configuration Manager > Protocols > IPX > Global

Default: If you disable the Multiple Host Address Enable parameter and enter a unique host number, the Configuration Manager assigns this number to all IPX interfaces you configure on the router.

Options: If you disable the Multiple Host Address Enable parameter and do *not* enter a router host ID number for this parameter, the Configuration Manager automatically generates a unique 6-byte host ID number for all IPX interfaces. The generated host ID is based on the serial number of the router's backplane.

Function: Any valid host number

Instructions: The router either uses this value as a host address for all IPX interfaces, or, if left empty, uses the backplane serial number as the host address for all interfaces (circuits).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.7

Caution: The IPX boxwide host address and the Token Ring MAC address must agree when the Multiple Host Address parameter is disabled.

Parameter: **Router Name**

Path: Configuration Manager > Protocols > IPX > Global

Default: None

Options: Any valid NetWare router or server name

Function: Specifies a symbolic name for the router. Any IPXWAN (RFC1634-compliant) interface in the node uses this name to identify itself to the IPX router or server at the opposite end of the WAN data link.

The symbolic name for the router must be unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a router or server name. It's a good idea to make the name meaningful to users as well as routers

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.15.1.9

Parameter:	**Primary Net Number (hex)**
Path:	Configuration Manager > Protocols > IPX > Global
Default:	None
Options:	The Primary Network Number (PNN) is a string of up to 8 hexadecimal characters.
Function:	Specifies an IPX network number for IPXWAN (RFC1634-compliant) link negotiation on all slots. The value of the PNN determines whether the local or remote WAN interface serves as IPX Link Master. The node with the highest PNN value becomes the IPX Link Master. The PNN should be unique among network numbers currently assigned.
Instructions:	Enter a unique network number for each node requiring one or more IPXWAN (RFC1634-compliant) interfaces. (This network number must be unique across the IPX network. Do not enter a number that a server is using as an internal network number, or a number that has been assigned on any segment in the network.) All unused values between 0x00000001 and 0xFFFFFFFD are valid values.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.15.1.5

IPX Advanced Global Parameters

IPX advanced global parameters enable you to fine tune the way IPX runs on the router. You access these parameters via the Edit IPX Advanced Global Parameters window (Figure A-4). To view all of the parameters in this window, you must click on the scroll bar.

Figure A-4. IPX Advanced Global Parameters Window

Parameter:	**Routing Method**
Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	Tick
Options:	Hop | Tick
Function:	Specifies for all slots the method of making IPX “best-route” decisions by: Ticks -- The amount of time, expressed in ticks, that a packet requires to reach another network segment. (Each tick = 1/18th of a second.) Hops -- The number of router hops a packet must traverse to reach another network segment. If you accept the default, Tick, and the router knows about two paths to a network, and both paths have equal tick values, the router chooses the path with the smallest number of hops. If you select Hop, and the best route results in the same number of hops, the router makes its decision based only on hops.
Instructions:	Choose the method that results in the best routing performance. Usually, the best route is the one with: The lowest number of ticks for a packet to reach a node on the destination network The lowest number of hops (if multiple routes exist with equal numbers of ticks for a packet to reach a node on the destination network) If routes exist with equal numbers of ticks and hops, choose either method. We recommend using the default (tick-based) method, because tick-based routing takes into account actual link delay in determining the best path between IPX networks. Thus, it provides a more accurate routing mechanism than simply “hop count.”
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.3

Parameter: Maximum Path

Path: Configuration Manager > Protocols > IPX > Global > Advanced
Default: 1 (path)
Range: 1 to 1,023 (paths)
Function: Specifies the maximum number of paths allowed for a given network destination and routing method.
Instructions: Accept the default (1) or specify an integer in the range 1 to 1,023.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.5

Parameter: Log Filter

Path: Configuration Manager > Protocols > IPX > Global > Advanced
Default: Trace
Options: None | Debug | Info | Trace | Debug Info | Debug Trace | Info Trace | Debug Info Trace
Function: Filters out the specified type of log message. For example, the default setting (Trace) filters out trace messages.
Instructions: Do not change the default value of this parameter unless you are an expert IPX user. Changing the value of this parameter produces significant boxwide effects on memory allocation within the router, and these changes can significantly affect router performance. If you are qualified as an expert user, enter a filtering mode that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.4

Parameter: Maximum Path Splits

Path: Configuration Manager > Protocols > IPX > Global > Advanced
Default: Enable
Options: Enable | Disable
Function: If enabled, IPX will do load balancing to a particular destination up to the number of paths specified in the Maximum Path parameter (see above).
Instructions: Accept the default (enable) to do load balance on the number of equal cost paths specified in the Maximum Path parameter above.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.6

Parameter: Maximum Hops

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 16 (hops)

Range: 1 to 255 (hops)

Function: Specifies the maximum number of hops an IPX packet may take to reach its destination.

Instructions: Accept the default (16) or specify an integer in the range 1 to 255. In the case of RIP, every node in the network should use the same Maximum Hops parameter value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.7

Parameter: Destination Count

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 0

Range: 0 to 5000 (destinations)

Function: Specifies the maximum number of destinations (networks) that the user expects the router to learn. IPX uses this value to preallocate table sizes for forwarding and network tables. If you specify zero, the default value, IPX dynamically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.17

Parameter: Service Count

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 1 (service)

Range: 1 to 5000 (services)

Function: Indicates the maximum number of services that the user expects the router to learn. IPX uses this value to preallocate table sizes for service tables. If you specify zero, the default value, IPX automatically allocates the amount of memory it needs for the tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.19

Parameter: Host Count

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: 1 (host)

Range: 1 to 5000 (hosts)

Function: Indicates the maximum next-hop hosts that the user expects the router to learn. IPX uses this value to preallocate table sizes for host tables. Changing this value can greatly affect the memory use by IPX, but it can also speed learning time for the router.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.21

Parameter:	**Aging Frequency**
Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	10 (seconds)
Range:	1 to the maximum positive integer (seconds)
Function:	Specifies the granularity, in seconds, for aging RIP and SAP information. IPX checks whether any routes have timed out every *n* seconds, where *n* is the interval that this parameter specifies.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.23

Parameter:	**Aging Pending Frequency**
Path:	Configuration Manager > Protocols > IPX > Global > Advanced
Default:	100 (routes and services)
Range:	1 to maximum positive integer (routes and services)
Function:	Specifies the number of routes and services to age (process) before pending. A higher number lets the aging process proceed more quickly.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.16.1.24

Parameter: **Default Route**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the use of the default route 0xFFFFFFFE for IPX routing.

Enable -- Directs the router to use the default route (if one exists in its routing table) when it receives an IPX packet that does not contain a known IPX destination address within the IPX protocol header.

Disable -- Forces the router to drop a packet whose destination address is unknown, even if a default route exists.

Instructions: Select Enable to allow IPX default routing.

Select Disable to turn off default routing.

MIB Object ID: .1.3.6.1.4.1.18.3.5.5.16.1.25

Parameter: **SAP via Default Route**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Disable

Options: Enable | Disable

Function: Indicates whether a SAP advertisement can be learned from an interface if the network number advertised in the SAP advertisement is unreachable, but a default route is accessible from that interface.

Enable -- Directs the router to accept a service if a direct or default route to the server is known.

Disable -- Accepts a service only if a direct route to the server advertising the service is known.

This feature gives you the option of making SAP entries available if the IPX default route is reachable.

Instructions: Select Enable to enable IPX default routing globally for SAP advertisements.

Select Disable to turn off default SAP advertisement routing.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.26

Note: Since it deviates from the IPX Default Route specification, enabling this feature may cause the interface to be incompatible with other router implementations.

Parameter: **Novell Certification Conformance**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Enable

Options: Enable | Disable

Function: Indicates whether you want the router to conform to Novell NetWare standards by propagating a NetBIOS Type 20 packet out of all its interfaces.

Instructions: Accept the default, Enable, if you want the router to propagate NetBIOS Type 20 packets out of all its interfaces (conforming to Novell standards). Select Disable if you have NetBIOS static routes configured and you want the router to direct a packet to its destination network. You must set the same option (Enable or Disable) for all routers in the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.15

Parameter: **GNS Response Mode**

Path: Configuration Manager > Protocols > IPX > Global > Advanced

Default: Alphabetical

Options: Alphabetical | Last Learned

Function: Determines the server to choose when responding to a get_nearest_server request.

Instructions: Accept the default to sort through all server names alphabetically.

Select Last Learned to choose the last server learned.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.16.1.29

IPX Interface Parameters

IPX interface parameters determine how IPX behaves on individual router interfaces. You access these parameters via the IPX Interfaces window (Figure A-5). To view all of the parameters in this window, you must click on the scroll bar.

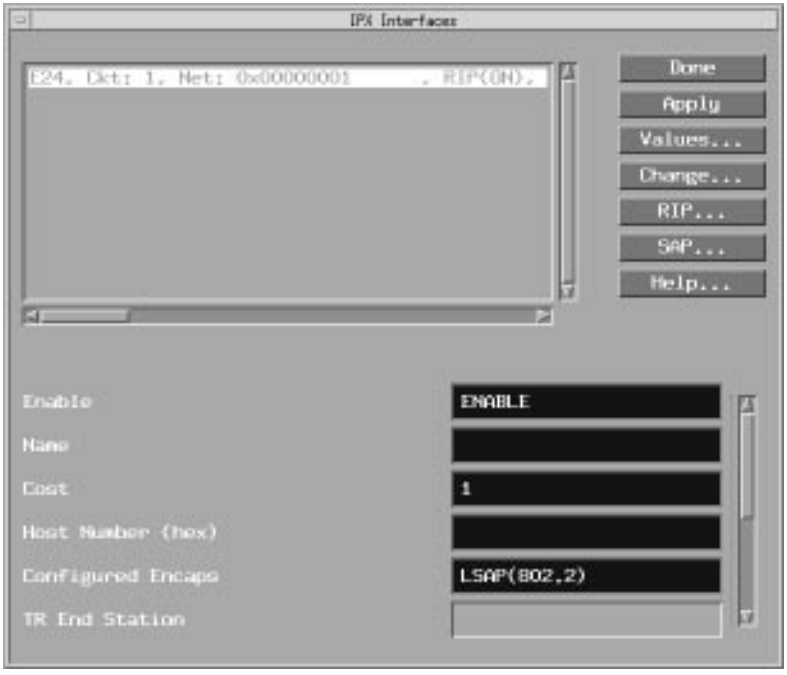

Figure A-5. IPX Interfaces Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPX routing on this interface.

Enable -- Initializes the IPX interface you added to a circuit. You can also use the Enable setting to reinitialize an existing disabled IPX interface. The actual operating state of an interface, once enabled, depends on

The current state of the associated circuit

The current state of the IPX global/slotwide protocol process

Disable -- Forces an IPX interface into the down (inoperative) state

Instructions: Select Enable if you previously set this parameter to Disable and now want to re-enable IPX routing on this interface.

Select Disable only if you want to disable IPX routing on this interface

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.2

Parameter: Name

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX server name

Function: Specifies a symbolic name for the interface.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a host, interface, router, or server name. It's a good idea to make the name meaningful to users as well as to routers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.7

Parameter: Cost

Path:	Configuration Manager > Protocols > IPX > Interfaces
Default:	1 (for hop- or tick-based routing)
Range:	1 to the maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Sets the cost (number of ticks or hops) for this interface. The cost is added to route information learned on this interface through RIP and is included in subsequent RIP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.38

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: None

Options: Any valid IPX host ID number

Function: If you enable Multiple Host Address Enable and want to accept the PROM-based default setting for the MAC Address Select circuit parameter, this IPX interface adopts a host number based on the MAC address of the underlying circuit. In this case, a PROM on the circuit supplies the number for the MAC address of the circuit and the host number of the interface.

You can enter a host number for this interface when:

- Multiple Host Addressing is enabled
- You do not want to accept the PROM-based (default) setting for MAC Address Select
- The circuit type supports only selective mode of operation (such as with Ethernet circuits)

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains effective for all other interfaces configured on the same circuit.)

You can enter a host number for this interface when the underlying circuit is Token Ring; see the instructions that follow.

Site Manager does not let you enter an IPX host number for any IPX interface if you first disable Multiple Host Address Enable in the IPX Global Parameters window

Instructions: Enter a value only if the circuit is not Token Ring and you want to assign a host number that is unique within the IPX internetwork to this IPX interface.

To set the host number of an IPX interface on a Token Ring circuit, you must change the MAC Address Select parameter for that circuit to CNFG (user-configured) and enter a MAC Address Override value for the circuit. The interface uses that value as its host number. This changes the circuit MAC address for all protocols configured on that Token Ring circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.25

Parameter: **Configured Encaps**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Circuit medium dependent

Options: Circuit medium dependent

Possible values: Ethernet | LSAP | Novell | SNAP | PPP

Function: Specifies the encapsulation methods (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, Token Ring, or sync). The encapsulation method supports communication on a specific logical network

Instructions: Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows:

Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.

Token ring circuits support LSAP and SNAP frames.

Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.

FDDI circuits support LSAP and SNAP frames.

HSSI circuits support PPP and SNAP Frames.

ISDN circuits support PPP frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter: **TR End Station**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables source routing on this interface. This parameter appears only when you add an IPX interface on a Token Ring circuit.

Instructions: Select Enable if this interface connects to a bridged Token Ring network. Select Disable only if you want to disable source routing over this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.59

Parameter: NetBIOS Accept

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables acceptance of all NetBIOS Type 20 (broadcast) packets received by this interface from an external source.

Instructions: Select Enable if you want this interface to accept all NetBIOS broadcast packets from an external source. Select Disable only if you want this interface to reject all NetBIOS broadcast packets from an external source.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.60

Parameter: NetBIOS Deliver

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables outbound delivery of all NetBIOS Type 20 (broadcast) packets received by this interface from another interface.

Instructions: Select Enable if you want to re-enable outbound delivery of NetBIOS broadcast packets received internally. Select Disable only to drop NetBIOS broadcast packets received internally.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.61

Parameter: **FR Broadcast (hex)**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0xFFFFFFFFFFFF (not displayed)

Options: Default value or a user-specified WAN broadcast address.

Function: Specifies a broadcast address for this IPX interface. (This parameter is available for any WAN protocol and any media type.)

Instructions: The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a WAN broadcast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

Leave blank to accept the default value or enter a WAN broadcast address to send all broadcast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all broadcast traffic through all logical connections associated with the IPX interface you are configuring. Broadcast traffic includes RIP and SAP broadcasts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.28

Parameter: **FR Multicast (hex)**

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0xFFFFFFFFFFFF (not displayed)

Options: Default value or a user-specified WAN multicast address.

Function: Specifies a multicast address for this IPX interface. (This parameter is available for any WAN protocol and any media type.)

The default value (0xFFFFFFFFFFFF) causes the data link layer to issue a multicast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

Instructions: Leave blank to accept the default value or enter a WAN multicast address to send all multicast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all multicast traffic through all logical connections associated with the IPX interface you are configuring.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.30

Parameter: IPX Watchdog Spoofing

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: Disable

Options: Enable | Disable

Function: Specifies whether a router can respond locally to broadcast IPX watchdog packets on behalf of clients that use dial-in connections. When you enable this parameter you also enable SPX Keep Alive Spoofing.

Instructions: Enable local watchdog packet acknowledgment to improve the efficiency of IPX wide-area links.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.64

Parameter: Delay

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0

Range: 0 to 2147483647

Function: Specifies the length of time, in microseconds, required to transmit 1 byte of data (excluding protocol headers) to a destination on the other end of this IPX circuit if the circuit is free of other traffic.

Instructions: Enter a value between 0 and 2147483647.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.66

Parameter: Stabilization Timer Delay (secs)

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: 120

Range: 0 to 2147483647

Function: Determines the amount of time, in seconds, that RIP/SAP waits before sending out initial route information when the dial-on-demand route first becomes enabled.

Instructions: The more routes that you expect a router to handle or the more dynamic the network is, the higher you should set this value to allow the router enough time to assimilate incoming routes before it sends out an initial update on a circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.69

Parameter: Throughput

Path: Configuration Manager > Protocols > IPX > Interfaces

Default: 0

Range: 0 to 2147483647

Function: Specifies the amount of data, in bits per second, that can flow through an IPX circuit if the circuit is free of other traffic.

Instructions: Enter a value between 0 and 2147483647.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.67

IPX Change Circuit Parameters

IPX change circuit parameters modify the way IPX runs over a particular circuit. You access these parameters via the IPX Change Circuit window (Figure A-6) for each circuit that you have configured .

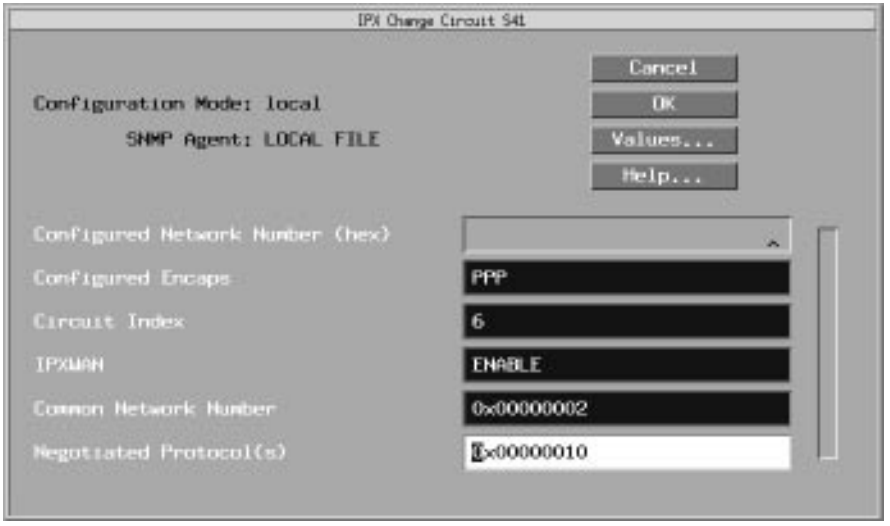

Figure A-6. IPX Change Circuit Window

Parameter:	**Configured Network Number (hex)**
Path:	Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change
Default:	None
Options:	Any valid IPX network number in hexadecimal format
Function:	Identifies the IPX network number that the user assigned to this IPX circuit. This parameter is active only for circuits that are not configured as IPXWAN interfaces or for those with the IPXWAN parameter explicitly disabled.
Instructions:	Enter a valid IPX network number in hexadecimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.22

Note: The Configured Network Number parameter is active only for circuits that are not configured as IPXWAN interfaces. The IPXWAN, Common Network Number, and Negotiated Protocols parameters appear only when the circuit is configured as an IPXWAN interface.

Parameter: Configured Encaps

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: Circuit medium dependent

Options: Circuit medium dependent

Possible values: Ethernet | LSAP | Novell | SNAP | PPP

Function: Specifies the encapsulation methods (such as Ethernet, PPP, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, Token Ring, or sync). The encapsulation method supports communication on a specific logical network.

Instructions: Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows:

- Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.
- Token ring circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21, T1/E1) support SNAP, PPP, and X.25 Point-to-Point (Ethernet) frames.
- FDDI circuits support LSAP and SNAP frames.
- HSSI circuits support PPP and SNAP frames.
- ISDN circuits support PPP frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.40

Parameter: Circuit Index

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: System-assigned

Options: Any valid circuit identifier

Function: Uniquely identifies this circuit within this instance of IPX.

Instructions: Accept the default or enter a valid circuit identifier.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.6

Parameter: IPXWAN

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPXWAN for this interface on this router. This parameter is active only for circuits that are configured as IPXWAN interfaces.

Instructions: Select Enable to turn on IPXWAN negotiation for this interface.

Select Disable to turn on IPXWAN negotiation for this interface.

MIB Object ID: Not Applicable

Parameter: Common Network Number (hex)

Path: Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change

Default: None

Options: Any valid IPX network number, 0x00000000 to 0xFFFFFFFD in hexadecimal format

Function: Specifies the IPX common network number assigned to this IPX circuit. This parameter is active only for circuits that are configured as IPXWAN interfaces that have the IPXWAN parameter enabled.

Instructions: Enter a valid IPX network number in hexadecimal format. Do not use the values 0xFFFFFFFE or 0xFFFFFFFF as network numbers. These values are reserved for system use.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.17.1.24

Parameter:	**Negotiated Protocol(s)**
Path:	Configuration Manager > Protocols > IPX > Interfaces > Circuit > Change
Default:	Unnumbered RIP
Options:	RIP | Unnumbered RIP
Function:	Indicates the protocol negotiated for this interface. This parameter is active only for circuits that are configured as IPXWAN interfaces and that have the IPXWAN parameter enabled.
Instructions:	Accept the default or click on Values to display the other choices. You can select more than one option. Click on the options you prefer, then click on OK to accept your choices. The parameter value appears as a hexadecimal number on the IPX Change Circuit window. The values are as follows: 0x00000008 RIP 0x00000010 Unnumbered RIP 0x00000018 RIP and Unnumbered RIP
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.17.1.8

IPX RIP Circuit Parameters

IPX RIP circuit parameters determine the way RIP behaves on a particular circuit. You access these parameters via the IPX RIP Circuit window (Figure A-7). To view all of the parameters in this window, you must click on the scroll bar.

Figure A-7. IPX RIP Circuit Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Enable

Options: Enable | Disable

Function: Specifies whether RIP is enabled on this IPX circuit.

Instructions: Select Enable to enable RIP on this circuit.

Select Disable to disable RIP on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.2

Note: If this parameter is set to Enable, a route filter can still prohibit the interface from updating its internal routing tables. See the description of route filtering in this chapter.

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Listen/Supply

Options: Listen/Supply | Listen | Supply

Function: Specifies the mode for this circuit.

Instructions: Select one of the following values:

Listen/Supply -- specifies that this interface both listens for and supplies RIP updates, as described in the following items.

Listen -- specifies whether this interface listens to RIP Periodic and Triggered updates from neighboring networks and conveys received routing information to its internal routing table.

Supply -- specifies whether the interface transmits all RIP Periodic and Triggered updates to routers in neighboring networks.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.6

Parameter: Pace

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP
Default: 18
Range: 0 to 1000
Function: Specifies the maximum pace (in packets per second) at which RIP packets can be sent on this circuit. A value of zero means that there is no limit on the pace.
Instructions: Accept the default or specify an integer value up to 1000.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.7

Parameter: Update Interval (sec)

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP
Default: 60
Range: 0 to 2678400
Function: Adjusts the frequency of RIP update packet transmissions, in seconds, for this circuit.
Instructions: The higher the number you enter, the less frequent the transmissions. If you enter zero, no periodic RIP updates are sent out over the IPX interface to the router. However, RIP immediate (one-time) update packets still propagate through the network, in compliance with Novell standards.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.8

Parameter: Age Multiplier

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP
Default: 3 (update interval increments)
Range: 1 to 6 (increments)
Function: Specifies the holding multiplier as the number of update intervals for information received in RIP periodic updates.
Instructions: Accept the default value or specify a value in the range 1 to 6. Increasing this value can cause routes to take longer to age out. Decreasing it could cause the router to age routes prematurely, if routing updates are missed. The combination of the update interval and age multiplier should be the same for all systems on a network segment.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.9

Parameter: Packet Size

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: 432

Options: Circuit-type dependent

Function: Specifies the maximum RIP packet size, in bytes, used on this circuit.

Instructions: Accept the default (432 bytes) unless you have a specific reason for specifying a different size packet. The packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.10

Parameter: Use Multicast

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Yes

Options: Yes | No

Function: Specifies whether to use a multicast address, configured with the Multicast Address parameter, to send RIP packets.

Instructions: Accept the default to allow multicast transmission of RIP packets.

Select No to disable multicast transmission of RIP packets

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.14

Parameter: Split Horizon

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Enable

Options: Enable │ Disable

Function: When generating RIP updates to be transmitted from an interface, the interface can exclude RIP routes learned on that interface.

Instructions: Select Enable if you previously set this parameter to Disable and now do not want the router to transmit RIP updates received from the interface over that same interface.

Select Disable only if you want the router to transmit RIP updates received from the interface over that same interface. Routes learned on that interface will be included in the RIP updates generated for that interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.15

Parameter: Immediate Update

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Enable

Options: Enable │ Disable

Function: When a change in status occurs for this circuit, immediately propagate that information to other routers in the internetwork.

Instructions: Accept the default. Enabling this parameter facilitates network traffic by letting routers know immediately about new or failed routes. When this parameter is disabled, other routers learn about such changes only at the next periodic update interval.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.17

Parameter: Default Route Supply

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Disable

Options: Enable | Disable

Function: If a default route exists in the routing table, this parameter specifies whether to advertise the default route, 0xFFFFFFE, in RIP packets.

Instructions: Select Enable to enable default route supply (that is, to advertise the default route) on this circuit.

Select Disable to disable default route supply (that is, not advertise the default route) on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.18

Parameter: Default Route Listen

Path: Configuration Manager > Protocols > IPX > Interfaces > RIP

Default: Disable

Options: Enable | Disable

Function: Specifies whether to accept the default route, 0xFFFFFFE, in RIP packets received on this circuit.

Instructions: Select Enable to accept the default route in RIP packets on this circuit.

Select Disable to reject the default route in RIP packets on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.32.1.19

IPX SAP Circuit Parameters

IPX SAP circuit parameters determine the way SAP works on a particular circuit. You access these parameters via the IPX SAP Circuit window (Figure A-8)

Figure A-8. IPX SAP Circuit Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Enable

Options: Enable | Disable

Function: Specifies whether SAP is enabled on this IPX circuit.

Instructions: Select Enable to enable SAP on this circuit.

Select Disable to disable SAP on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.2

Note: If this parameter is set to Enable, a SAP filter can still prohibit the interface from updating its internal SAP tables. See the description of SAP filtering in Chapter 5.

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Listen/Supply

Options: Listen/Supply | Listen | Supply

Function: Specifies the mode for this circuit.

Instructions: Select one of the following values:

Listen/Supply -- specifies that this interface both listens for and supplies SAP updates, as described in the following items.

Listen -- specifies whether this interface listens to SAP Periodic and Triggered updates from neighboring networks and conveys received SAP services information to its internal SAP services table.

Supply -- specifies whether the interface transmits all SAP Periodic and Triggered updates to routers in neighboring networks.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.6

Parameter: Pace

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 18

Range: 0 to 1000

Function: Specifies the maximum pace (in packets per second) at which SAP packets can be sent on this circuit. A value of zero means that there is no limit on the pace.

Instructions: Accept the default or specify an integer value up to 1000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.7

Parameter: Update Interval (sec)

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 60

Range: 0 to 2678400

Function: Adjusts the frequency, in seconds, of SAP update packet transmissions for this circuit.

Instructions: The higher the number you enter, the less frequent the transmissions. If you enter zero, no periodic updates are sent out over the IPX interface to the router. However, SAP immediate (one-time) updates still propagate through the network, in compliance with Novell standards.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.8

Parameter: Age Multiplier

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 3 (update interval increments)

Range: 1 to 6 (increments)

Function: Specifies the holding multiplier, in update interval increments, for information received in SAP periodic updates.

Instructions: Accept the default value or specify a value in the range 1 to 6. Increasing this value can cause routes to take longer to age out. Decreasing it could cause the router to age routes prematurely, if routing updates are missed. The combination of the update interval and age multiplier should be the same for all systems on a network segment.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.9

Parameter: **Packet Size**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: 480

Options: Circuit-type dependent

Function: Specifies the maximum SAP packet size, in bytes, used on this circuit.

Instructions: Accept the default (480 bytes) unless you have a specific reason for specifying a different size packet. The packet size plus the IPX header (30 bytes) cannot exceed the MTU of the link.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.10

Parameter: **Nearest Server Reply**

Path: Configuration Manager Protocols > IPX > Interfaces > SAP

Default: Yes

Options: Yes | No

Function: Specifies whether to respond to SAP *get_nearest_server* requests.

Instructions: Accept the default to allow this router to respond to a SAP *get_nearest_server* request. If you have disabled split horizon, you may want to set this parameter to No.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.11

Parameter: **Use Multicast**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Yes

Options: Yes | No

Function: Specifies whether to use a multicast address to send SAP packets.

Instructions: Accept the default to allow multicast transmission of SAP packets.

Select No to disable multicast transmission of SAP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.16

Parameter: **Save Full Name**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Yes

Options: Yes | No

Function: Determines whether the router will save all 48 bytes in the service name field of SAP packets or if it will ignore all characters after the null character when a service field name is less than 48 bytes.

Instructions: Accept the default to save all 48 bytes in the service name field of SAP packets.

Select No to ignore all characters after the null character.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.20

Parameter: **Split Horizon**

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Enable

Options: Enable | Disable

Function: When generating SAP updates to be transmitted from an interface, the interface can exclude SAP servers learned on that interface.

Instructions: Select Enable if you previously set this parameter to Disable and now do not want the router to transmit SAP updates received from the interface over that same interface.

Select Disable only if you want the router to transmit SAP updates received from the interface over that same interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.17

Parameter: Immediate Update

Path: Configuration Manager > Protocols > IPX > Interfaces > SAP

Default: Enable

Options: Enable | Disable

Function: When a change in status occurs for this circuit, immediately propagate that information to other routers in the internetwork.

Instructions: Accept the default. Enabling this parameter facilitates network traffic by letting routers know immediately about new or failed services. When this parameter is disabled, other routers learn about such changes only at the next periodic update interval.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.33.1.19

IPX NetBIOS Static Route Configuration Parameters

IPX NetBIOS static route configuration parameters establish a NetBIOS Static Route.You access these parameters via the IPX NetBIOS static route configuration window (Figure A-9).

Figure A-9. IPX NetBIOS Static Route Configuration Window

Parameter: Target Server

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes > Add

Default: None

Options: The name of a NetBIOS target server, specified as a string of up to 16 alphanumeric characters (which can include wildcards and pattern-matching characters). You can include any printable character, including $, #, and so on. To specify a backslash, enter two backslashes (\\). You can also use the hexadecimal equivalent (*xx*) of any valid ASCII character. For example, you can specify \20 for space or \21 for ! (note that *xx* counts as one character).

Function: Specifies the name of the NetBIOS server.

Instructions: Enter the name or part of the name of the NetBIOS server. The name can be up to 16 alphanumeric characters. For a list of the wildcards and pattern-matching characters, refer to Table 5-1 on page 5-59.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.4

Note: You cannot change the Target Server parameter once you set it.only in the IPX NetBIOS Static Route Configuration window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes > Add

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.5

Note: The Configuration Manager does not let you reconfigure the Target Server parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route. However, you can reconfigure all other parameters associated with a static route.

IPX NetBIOS Static Route Parameters

IPX NetBIOS static route parameters determine the location of a NetBIOS static route.You access these parameters via the IPX NetBIOS static route configuration window (Figure A-10).

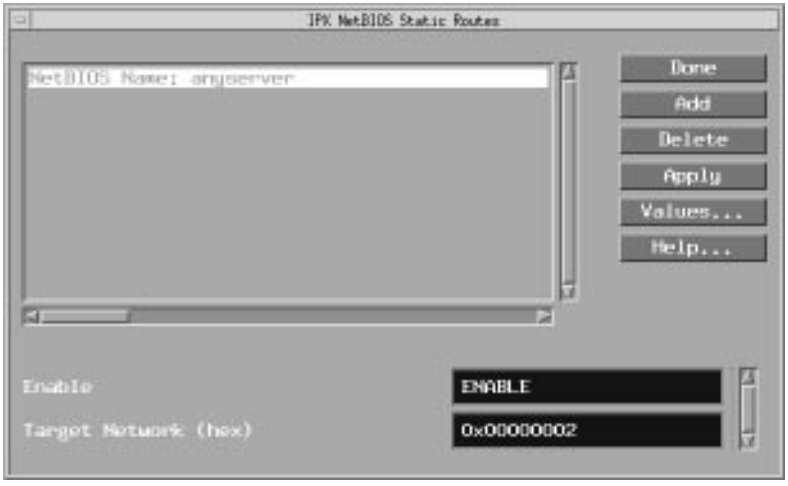

Figure A-10. IPX NetBIOS Static Routes Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes

Default: Enable

Options: Enable | Disable

Function: Specifies the state (active or inactive) of the static route record in the NetBIOS routing table.

Instructions: Select Disable to make the static route record inactive in the NetBIOS routing table.

Select Enable to make the static route record active in the NetBIOS routing table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.2

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > NetBIOS Static Routes

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.27.1.5

Adjacent Hosts Configuration Parameters

IPX adjacent hosts configuration parameters establish an adjacent host. You access these parameters via the IPX Adjacent Hosts configuration window (Figure A-11).

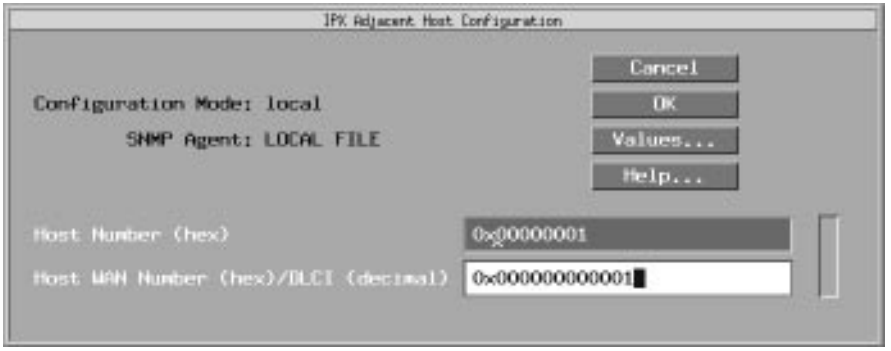

Figure A-11. IPX Adjacent Hosts Configuration Window

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: None

Options: Valid host ID of the adjacent host

Function: Specifies the host ID of the adjacent host.

Instructions: Enter a host ID of up to 12 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.5

Parameter: Host WAN Address (hex)/DLCI (decimal)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts > Add

Default: None

Options: WAN Address | Data Link Connection Identifier

Function: Lets you enter a WAN address or a DLCI. The format depends on the underlying data link protocol type.

Instructions: Enter a WAN address of up to 16 hexadecimal characters if the interface is on an ATM or SMDS network

Enter a decimal DLCI number if the interface is on a Frame Relay network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.6

IPX Adjacent Hosts Parameters

IPX adjacent hosts parameters determine the location of an adjacent host. You access these parameters via the IPX Adjacent Hosts window (Figure A-12).

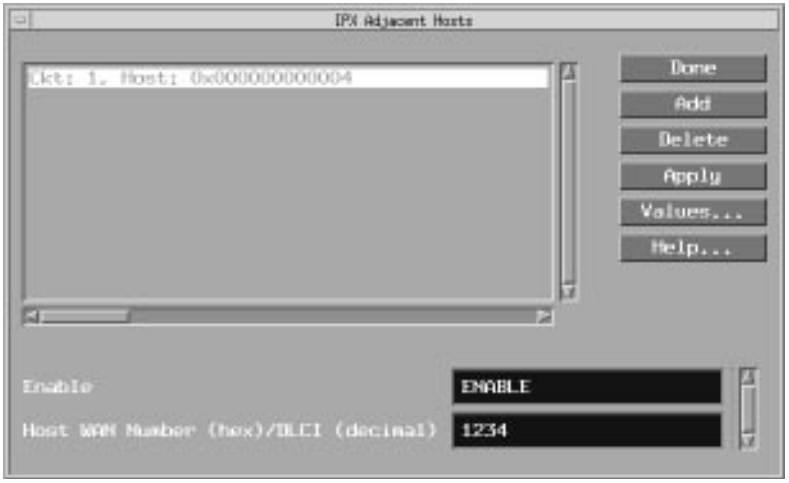

Figure A-12. IPX Adjacent Hosts Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts

Default: Enable

Options: Enable | Disable

Function: Sets the state (active or inactive) of the adjacent host record in the IPX routing tables.

Instructions: Select Disable to make the adjacent host record inactive in the IPX host table.

Select Enable to make the adjacent host record active in the IPX host table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.2

Parameter:	**Host WAN Address (hex)/DLCI (decimal)**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Adj. Hosts
Default:	None
Options:	WAN Address | Data Link Connection Identifier
Function:	Lets you enter a WAN address or a DLCI. The format depends on the underlying data link protocol type.
Instructions:	Enter a WAN address of up to 16 hexadecimal characters if the interface is on an ATM or SMDS network. Enter a decimal DLCI number if the interface is on a Frame Relay network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.26.1.6

IPX Static Route Configuration Parameters

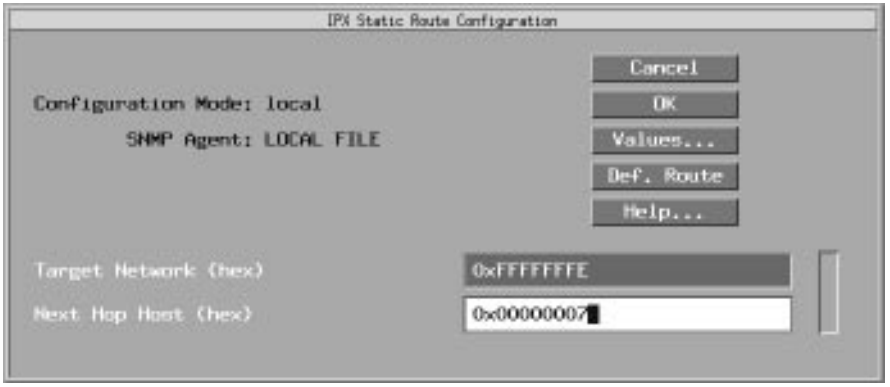

Figure A-13. IPX Static Route Configuration Window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of the network to which you want to configure the static route.

Instructions: Enter a network address of up to 8 hexadecimal characters or click on Def. Route to have the Configuration Manager fill in the default route 0xFFFFFFFE.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.5

Note: The Configuration Manager does not let you reconfigure the Target Network parameter for a static route. If you want to change this parameter, you must delete the static route and add a new route with the proper information. However, you can reconfigure all other parameters associated with a static route.

Parameter: Next Hop (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: None

Options: Any valid host address in hexadecimal notation

Function: Specifies the address of the next-hop host in the static routing path.

Instructions: Enter a host address of up to 12 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.8

Parameter: Hop Count

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: 0

Range: 0 to the value of the Maximum Hops parameter, minus 1

Function: The IPX router uses Hop Count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means “use the hop count associated with the interface.”

Instructions: Accept the default (0) or enter a value from 1 to one less than the maximum number of hops.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.7

Parameter: Ticks

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route > Add

Default: 0

Range: 0 to maximum positive integer

Function: Specifies the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.”

Instructions: Accept the default value (0) or enter a value from 1 to the maximum positive integer.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.6

IPX Static Route Parameter Descriptions

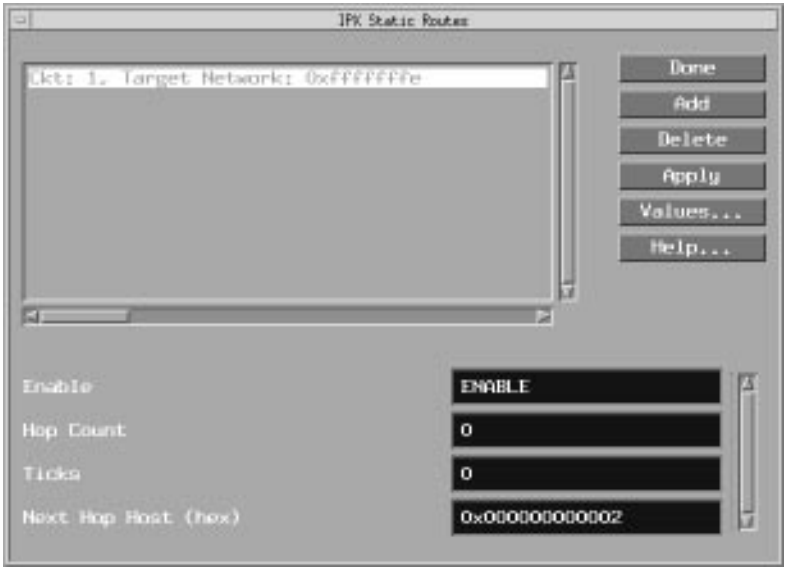

Figure A-14. IPX Static Routes Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route

Default: Enable

Options: Enable | Disable

Function: Specifies the state (active or inactive) of the static route record in the IPX routing tables.

Instructions: Select Disable to make the static route record inactive in the IPX routing table.

Select Enable to make the static route record active in the IPX routing table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.2

Parameter: Hop Count

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route
Default: 0
Range: 0 to the value of the Maximum Hops parameter, minus 1
Function: The IPX router uses Hop Count when determining the best route for a datagram to follow. The hop count is also propagated through RIP. The default setting of 0 for static routes means “use the hop count associated with the interface.”
Instructions: Accept the default (0) or enter a value from 1 to one less than the maximum number of hops.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.7

Parameter: Ticks

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route
Default: 0
Range: 0 to maximum positive integer
Function: Specifies the number of 1/18th-second timer ticks required for an IPX datagram to traverse this static route. The IPX router uses tick cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes means “use the tick count associated with the interface.”
Instructions: Accept the default value (0) or enter a value from 1 to the maximum positive integer.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.6

Parameter: Next Hop Host (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Route
Default: None
Options: Any valid host address in hexadecimal notation
Function: Specifies the address of the next-hop host in the static routing path.
Instructions: Enter a host address of up to 12 hexadecimal characters.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.19.1.8

IPX Static Service Configuration Parameters

This section describes all parameters shown in the IPX Static Service Configuration window.

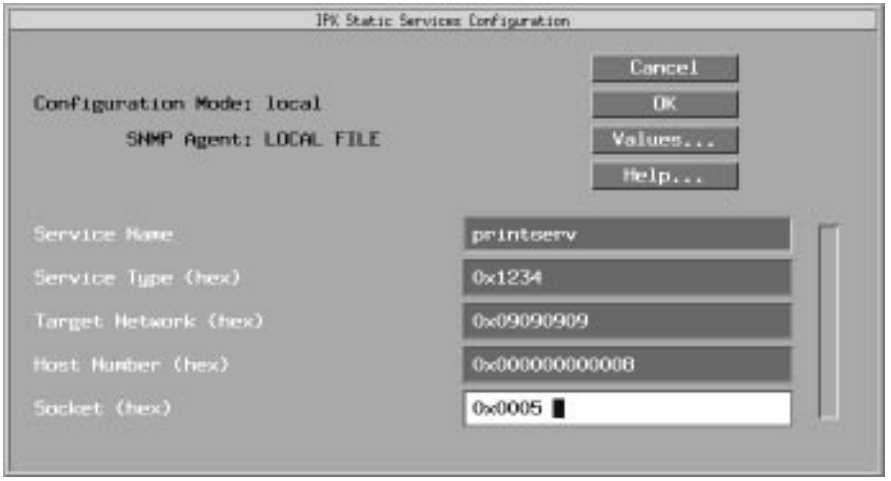

Figure A-15. IPX Static Service Configuration Window

Parameter: Service Name

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: Any valid Novell NetWare server name

Function: Assigns a symbolic name to the service you want to advertise.

Instructions: Use the *actual* name of the server that the clients will attach to. It helps if this is a name meaningful to the network administrator. The name must be unique among all names assigned to IPX servers of the same type on the IPX internetwork.

See the documentation that came with your NetWare operating system for guidelines on specifying a server name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.5

Parameter: **Service Type (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format. (The number must be a value between 0x0001 and 0xFFFE, inclusive.)

Function: Specifies the type of service to advertise from the associated IPX (LAN) interface (for example, 0x0004 for fileserver, 0x0007 for printerserver).

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading zeros.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.6

Parameter: **Target Network (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: Any valid IPX network address in hexadecimal notation.

Function: Specifies the network address of this service.

Instructions: Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing table. The entry can be learned dynamically by the router, or you can configure the entry as a static route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.7

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv. > Add

Default: None

Options: The address (host ID) of the service.

Function: Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Instructions: Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server. (For example, most NetWare Server host IDs are usually 0x000000000001.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.8

Parameter: Socket (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Add

Default: None

Options: Any valid socket address. (The number must have a value between 0x0001 and 0xFFFE, inclusive.)

Function: Specifies the socket address of this service.

Instructions: Enter any valid socket address consisting of up to 4 hexadecimal characters (for example, 0x0451).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.9

Note: Refer to Appendix C for a list of common service types (current as of the publication date of this manual).

IPX Static Service Parameters

Note: The Configuration Manager does not let you change the Service Name or Type parameters you set when you added the static service. To establish new values for these parameters for a particular static service, you must delete that service and configure a new service. You can, however, reconfigure all other parameters associated with a static service.

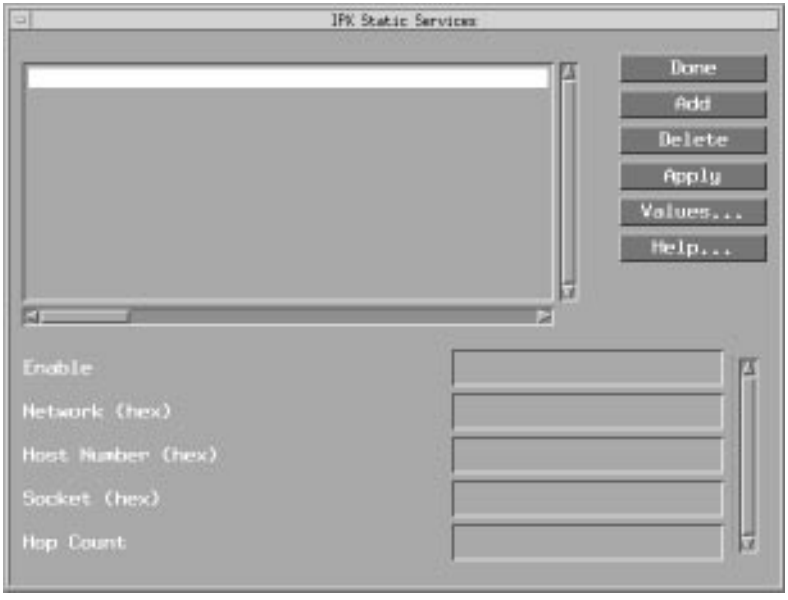

Figure A-16. IPX Static Services Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: Enable

Options: Enable | Disable

Function: Enables or disables a static service previously added to a specific IPX interface.

Instructions: Select Enable to re-enable a static service previously disabled. This restores client access to NetWare services configured earlier on the IPX interface.

Disable a static service to make NetWare services configured earlier unavailable to clients.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.2

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: None

Options: Any valid IPX network address in hexadecimal notation.

Function: Specifies the network address of this service.

Instructions: Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing table. The entry can be learned dynamically by the router, or you can configure the entry as a static route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.7

Parameter: Host Number (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: None

Options: The address (host ID) of the service.

Function: Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Instructions: Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.8

Parameter: Socket (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: None

Options: Any valid socket address. (The number must have a value between 0x0001 and 0xFFFE, inclusive.)

Function: Specifies the socket address of this service.

Instructions: Enter any valid socket address consisting of up to 4 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.23.1.9

Parameter: Hop Count

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Static Serv

Default: None

Options: Any valid number of hops, from 1 to the value of the Maximum Hops parameter, minus 1

Function: Specifies the number of subsequent router hops required from this router to reach a specific remote Novell server or service.

Instructions: Enter the number of router hops that exist between the router and the service you want to advertise.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.10

Route Filter Configuration Parameters

This section describes all parameters shown in the IPX Route Filter Configuration window.

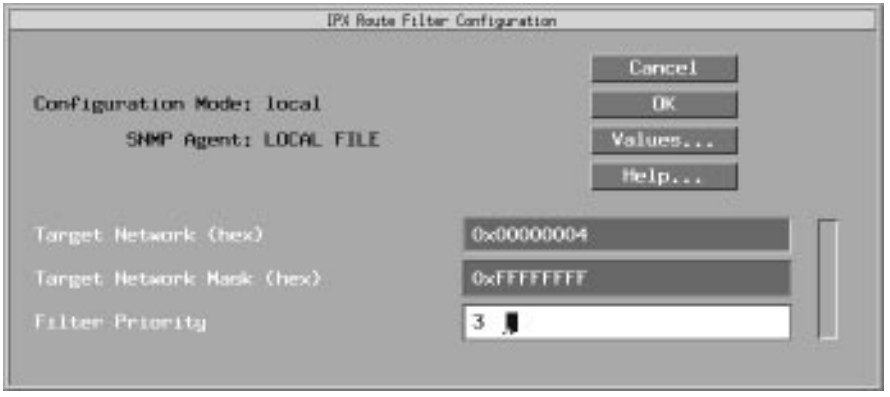

Figure A-17. IPX Route Filter Configuration Window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter > Add

Default: None

Options: Any valid NetWare address in hexadecimal format

Function: Identifies the network on which you want to apply the filter (the “filter ID” in the previous example).

Instructions: Enter the address of the target network in hexadecimal format. Using a mask, you can make this stand for a single ID or for a range of IDs with similar addresses. You can select all IDs by entering the wildcard value 0xFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.6

Parameter: Target Network Mask (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter > Add

Default: None

Range: 0x00000000 to 0xFFFFFFFF

Function: Specifies the mask that you want to apply.

Instructions: Enter 8 hexadecimal characters.

The character F in the mask definition requires an exact match with the corresponding character in the filter ID.

The mask character 0 matches any alphanumeric character.

You can combine the F and 0 characters in any order in the mask to filter any combination of network addressing schemes used within the IPX internetwork.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter > Add

Default: None

Range: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.13

IPX Route Filter Parameters

This section describes how to set all the parameters shown on the IPX Route Filters window.

Figure A-18. IPX Route Filters Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: Enable

Options: Enable | Disable

Function: Enables or disables a route filter previously added to a specific IPX interface.

Instructions: Select Enable to enable a route filter.

Select Disable to disable a route filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.2

Parameter: **Target Network (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: None

Options: Any valid NetWare address in hexadecimal format

Function: Identifies the network on which you want to apply the filter (that is, the “filter ID” in the previous example).

Instructions: Enter the address of the target network in hexadecimal format. Using a filter, you can make this stand for a single ID or for a range of IDs with similar addresses. You can select all IDs by entering the wildcard value 0xFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.6

Parameter: **Target Network Mask (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: None

Range: 0x00000000 to 0xFFFFFFFF

Function: Specifies the mask that you want to apply.

Instructions: Enter 8 hexadecimal characters.

The character F in the mask definition requires an exact match with the corresponding character in the filter ID.

The mask character 0 matches any alphanumeric character.

You can combine the F and 0 characters in any order in the mask to filter any combination of network addressing schemes used within the IPX internetwork.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: None

Range: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.13

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: Outbound

Options: Outbound | Inbound | Both

Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.

Instructions: Specify Inbound if you want to apply the filter to RIP packets coming into this interface.

Specify Both if you want to filter both inbound and outbound packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.8

Parameter: Protocol

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Route Filter

Default: Any

Options: Any | Local | RIP | Static

Function: Applies this filter only to routes learned on the specified protocol when sending RIP updates. This does not apply to Inbound routes.

Instructions: Specify the protocol on which you want to apply the filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.10

Parameter:	**Action**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any RIP advertisement that matches the route filter criteria you established.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement or acceptance of routes that match the specified route filter criteria. Select Suppress to configure the IPX router to drop RIP advertisements that match the specified route filter criteria.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.29.1.9

Parameter: Cost

Path: Configuration Manager > Protocols > IPX > Static/Filter Table > Route Filter

Default: 1 (for hop- or tick-based routing)

Range: 1 to maximum positive integer (if tick-based routing is enabled)

1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)

Function: Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent RIP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user. Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

If the filter is an *inbound* filter, the entered cost replaces the cost associated with the route in the RIP advertisement, and the router uses this cost in its calculations.

If this is an *outbound* filter, the entered cost replaces the route's cost that this router advertises in RIP packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.29.1.11

Service Network Filter Configuration Parameters

This section describes all parameters shown in the IPX Service Network Filter Configuration window.

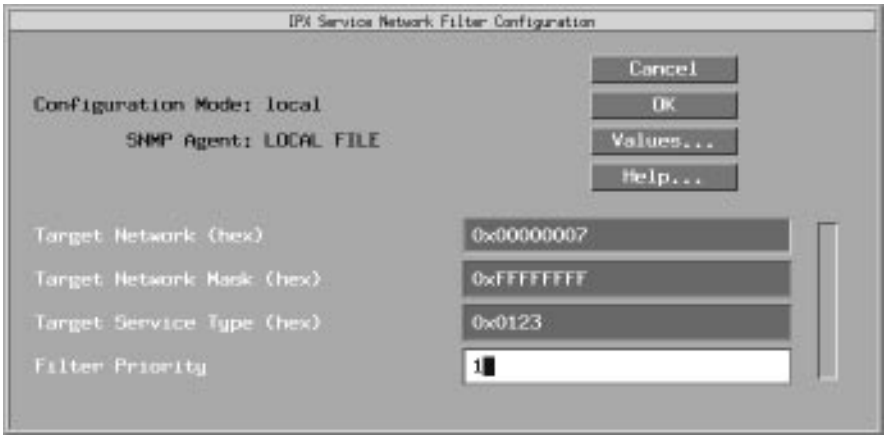

Figure A-19. IPX Service Network Filter Configuration Window

Parameter: Target Network (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Options: Any valid network address in hexadecimal notation.

Function: Specifies the network that you want to filter. The value 0xFFFFFFFF specifies all networks.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.6

Parameter: Target Network Mask (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: The mask, combined with the Target Network parameter value, determines which networks will be filtered.

Instructions: Enter a network address or filter pattern of up to 8 hexadecimal characters. A mask of 0xFFFFFFFF specifies an exact match with the network address specified in the Target Network parameter. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.7

Parameter: Target Service Type (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format

Function: Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid server types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.8

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter > Add

Default: None

Range: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.14

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Outbound

Options: Outbound │ Inbound │ Both

Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.

Instructions: Specify Inbound if you want to apply the filter to SAP packets coming into this interface.

Specify Both if you want to filter both inbound and outbound packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.9

IPX Service Network Filter Parameters

This section describes all parameters shown in the IPX Service Network Filters window.

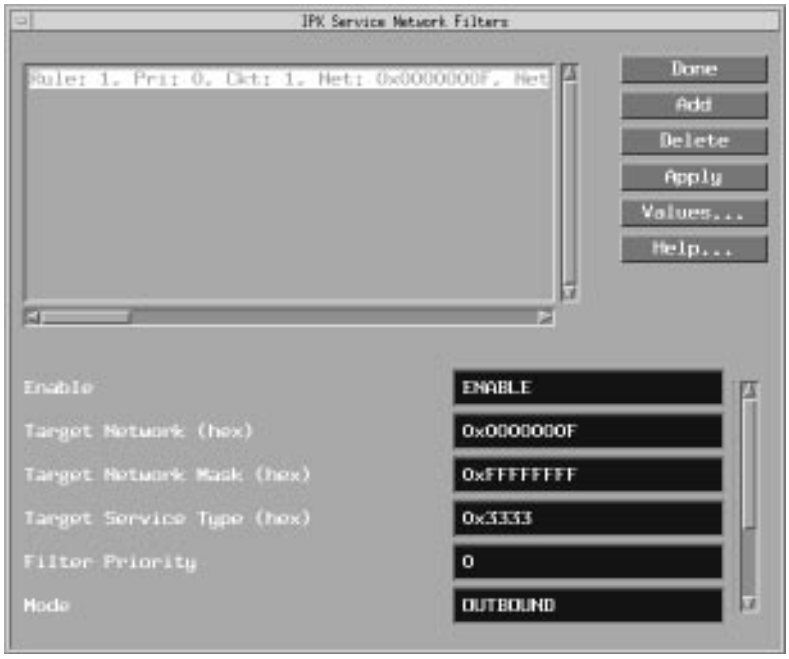

Figure A-20. IPX Service Network Filters Window

Parameter: **Enable**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Enable

Options: Enable | Disable

Function: Specifies whether the service network filter displayed is active on this interface.

Instructions: Select Enable to enable the service network filter.

Select Disable to disable the service network filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.2

Parameter: **Target Network (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: Any valid NetWare address in hexadecimal notation

Function: Specifies the network on which you want to apply the service network filter.

Instructions: Enter the address of the target network in hexadecimal format. Using a mask, you can make this stand for a single network or a range of networks with similar addresses. You can specify all networks by entering a Target Network of 0xFFFFFFF and a Target Network Mask of 0xFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.6

Parameter: **Target Network Mask (hex)**

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: The mask, combined with the Target Network parameter value, determines which networks will be filtered.

Instructions: Enter a network address or filter pattern of up to 8 hexadecimal characters. A mask of 0xFFFFFFFF specifies an exact match with the network address specified in the Target Network parameter. You can specify all networks by entering a Target Network of 0xFFFFFFFF and a Target Network Mask of 0xFFFFFFFF. A value of 0x0 is invalid.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.7

Parameter: Target Service Type (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format

Function: Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading zeros. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid server types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.8

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: None

Range: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.14

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Outbound

Options: Outbound | Inbound | Both

Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.

Instructions: Specify Inbound if you want to apply the filter to SAP packets coming into this interface.

Specify Both if you want to filter both inbound and outbound packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.9

Parameter: Protocol

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Any

Options: Any │ Local │ Static │ SAP

Function: Applies this outbound filter only to services learned on the specified protocol when sending SAP updates. This does not apply to inbound services.

Instructions: Specify the protocol on which you want to apply the filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.11

Parameter: Action

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter

Default: Advertise/Accept

Options: Advertise/Accept │ Suppress

Function: Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Target Network and Target Service Type parameters.

Instructions: Select Advertise/Accept to enable the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Target Network and Target Service Type parameters.

Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Target Network and Target Service Type parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.30.1.10

Parameter:	**Cost**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Net Filter
Default:	1 (for hop- or tick-based routing)
Options:	1 to maximum positive integer (if tick-based routing is enabled) 1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)
Function:	Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent SAP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.
Instructions:	Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router. If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in SAP advertisements sent from this router. If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.30.1.12

IPX Service Name Filter Configuration Parameters

This section describes all parameters shown in the IPX Service Name Filter Configuration window.

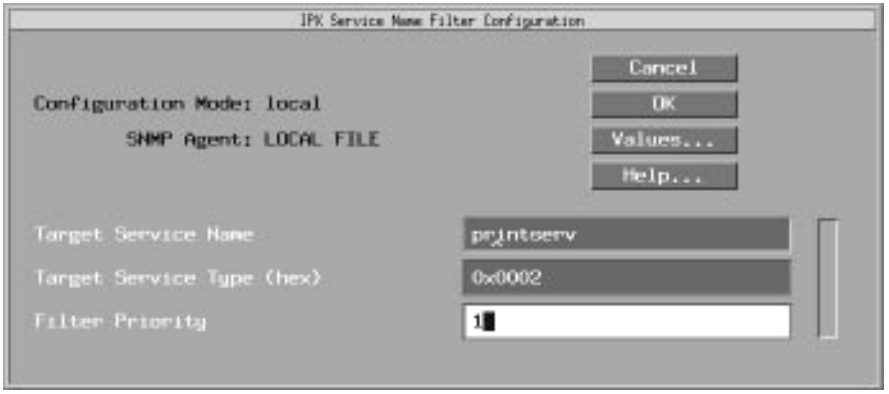

Figure A-21. IPX Service Name Filter Configuration Window

Parameter: Target Server Name

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Service Name Filters

Default: None

Options: Any valid alphanumeric server name or one containing wildcard characters or a pattern-matching regular expression

Function: This is the filter that you want to apply. It can specify the name of the server to which you are applying the service name filter, or it can be a filter containing a wildcard or a pattern (regular expression) to be matched. (See “Using Wildcards with SAP Filters” and “Using Pattern Matching with SAP Filters” for lists of these characters.)

Instructions: Enter a service name or filter pattern consisting of up to 48 alphanumeric characters, optionally including wildcards or a regular expression (pattern).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.6

Parameter: Target Service Type (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Service Name Filters

Default: None

Options: Any valid Novell service type number in 4-digit hexadecimal format

Function: Specifies the type of service that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the service type number in 4-digit hexadecimal format. Include leading zeros. For all types, enter a value of FFFF. See Appendix A for a list of valid service types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Service Name Filters

Default: None

Range: 0 to the maximum positive integer

Function: Specifies the priority of this filter in relation to other filters of the same type.

Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.13

IPX Service Name Filter Parameters

This section describes how to set all parameters shown on the IPX Service Name Filters window.

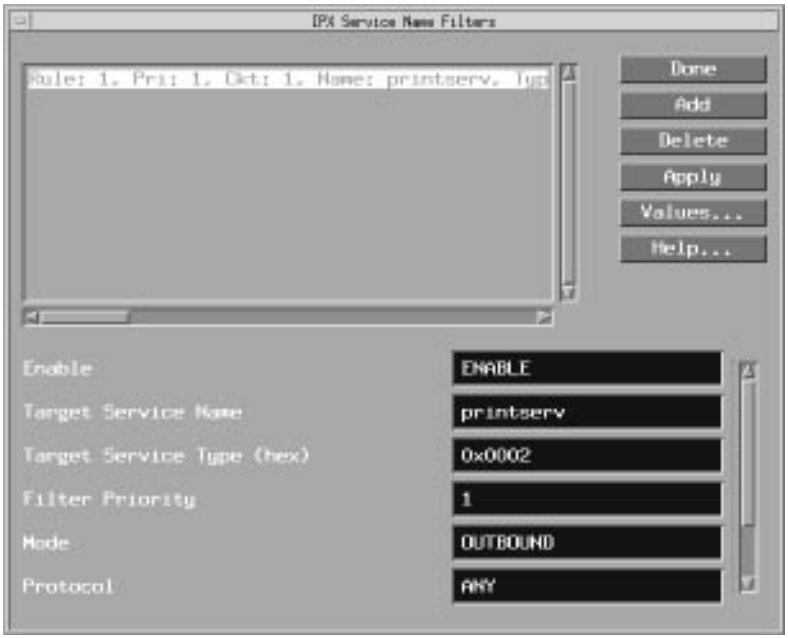

Figure A-22. IPX Service Name Filters Window

Parameter: Enable

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: Enable

Options: Enable | Disable

Function: Specifies whether the service name filter displayed is active on this interface.

Instructions: Select Enable to enable the service name filter.

Select Disable to disable the service name filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.2

Parameter: Target Server

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: None

Options: Any valid alphanumeric server name or one containing wildcard characters or a pattern-matching regular expression. (See “Using Wildcards with SAP Filters” and “Using Pattern Matching with SAP Filters” for lists of these characters.)

Function: This is the filter that you want to apply. It can specify the name of the server to which you are applying the server-level SAP filter, or it can be a filter containing a wildcard or a pattern (regular expression) to be matched.

Instructions: Enter a service name or filter pattern consisting of up to 48 alphanumeric characters, optionally including wildcards or a regular expression (pattern).

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.6

Parameter: Target Service Type (hex)

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format

Function: Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of 0xFFFF. See Appendix A for a list of valid service types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.7

Parameter: Filter Priority

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter
Default: None
Range: 0 to the maximum positive integer
Function: Specifies the priority of this filter in relation to other filters of the same type.
Instructions: Enter a decimal value that indicates this filter's priority relative to other filters of the same type for this interface. Lower values indicate higher priorities. (The highest priority is 0.)
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.13

Parameter: Mode

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter
Default: Outbound
Options: Outbound │ Inbound │ Both
Function: Specifies whether you want to apply the filter to inbound packets, outbound packets, or both.
Instructions: Accept the default, Outbound, if you want to apply the filter to SAP packets advertised by the specified interface.

Specify Inbound if you want to apply the filter to SAP packets coming into this interface.

Specify Both if you want to filter both inbound and outbound packets.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.8

Parameter: Protocol

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter
Default: Any
Options: Any │ Local │ Static │ SAP
Function: Applies this outbound filter only to services learned on the specified protocol when sending SAP updates. This does not apply to inbound services.
Instructions: Specify the protocol on which you want to apply the filter.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.10

Parameter:	**Action**
Path:	Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter
Default:	Advertise/Accept
Options:	Advertise/Accept | Suppress
Function:	Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Target Service Name and Target Service Type parameters.
Instructions:	Select Advertise/Accept to enable the filter to allow advertisement or acceptance of services that match the filter criteria you established in the Service Name and Service Type parameters. Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Service Name and Service Type parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.31.1.9

Parameter: Cost

Path: Configuration Manager > Protocols > IPX > Static/Filter Tables > Name Filter

Default: 1 (for hop- or tick-based routing)

Options: 1 to maximum positive integer (if tick-based routing is enabled)

1 to one less than the value specified in the Maximum Hops parameter (if hop-based routing is enabled)

Function: Used only when the Action parameter is Advertise/Accept, this parameter assigns a cost for routes matching this filter. A zero cost indicates that the route's actual cost should be used. This parameter sets the cost (number of ticks or hops) for this interface. The cost is included in subsequent SAP packets sent to other interfaces. IPX disposes of the packet when its hop count passes a value that is one less than the value of the Maximum Hops parameter. This value must be the same across the network.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Technical Response Center engineer). Changing the value of this parameter can significantly affect router performance. If you are qualified as an expert user, enter a value that yields a level of performance most appropriate for network applications supported by this router.

If the filter is an *inbound* filter, the entered cost replaces the cost associated with the server in the SAP advertisement, and the router uses this cost in its calculations.

If this is an *outbound* filter, the entered cost replaces the server's cost that is advertised in SAP packets by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.31.1.11

Appendix B
IPX Default Parameter Settings

This appendix lists the default settings for IPX parameters. Use the Configuration Manager to edit any of the default settings listed here.

IPX Global Parameter Defaults

This section describes all parameters shown on the Edit IPX Global Parameters window.

Table B-1. IPX Global Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.15.1.2
Multiple Host Address Enable	Enable	1.3.6.1.4.1.18.3.5.5.15.1.6
Host Number (hex)	If you disable the Multiple Host Address Enable parameter and enter a unique host number, the Configuration Manager assigns this number to all IPX interfaces you configure on the router. If you disable the Multiple Host Address Enable parameter and do not enter a boxwide host ID number for this parameter, the Configuration Manager automatically generates a unique 6-byte host ID number for all IPX interfaces, based on the serial number of the router's backplane.	1.3.6.1.4.1.18.3.5.5.15.1.7
Router Name	None	1.3.6.1.4.1.18.3.5.5.15.1.9
Primary Net Number (hex)	None	1.3.6.1.4.1.18.3.5.5.15.1.5

IPX Advanced Global Parameter Default Values

This section describes all parameters shown on the Edit IPX Advanced Global Parameters window.

Table B-2. IPX Advanced Global Parameter Default Values

Parameter	Default	MIB Object ID
Routing Method	Tick	1.3.6.1.4.1.18.3.5.5.16.1.3
Maximum Path	1 (path)	1.3.6.1.4.1.18.3.5.5.16.1.5
Log Filter	Trace	1.3.6.1.4.1.18.3.5.5.16.1.4
Maximum Path Splits	Enable	1.3.6.1.4.1.18.3.5.5.16.1.6
Maximum Hops	1 (hop)	1.3.6.1.4.1.18.3.5.5.16.1.7
Destination Count	1 (destination)	1.3.6.1.4.1.18.3.5.5.16.1.17
Service Count	1 (service)	1.3.6.1.4.1.18.3.5.5.16.1.1
Host Count	1 (host)	1.3.6.1.4.1.18.3.5.5.16.1.21
Aging Frequency	10 (seconds)	1.3.6.1.4.1.18.3.5.5.16.1.23
Aging Pending Frequency	100 (routes and services)	1.3.6.1.4.1.18.3.5.5.16.1.24
Default Route	Enable	1.3.6.1.4.1.18.3.5.5.16.1.25
SAP Via Default Route	Disable	1.3.6.1.4.1.18.3.5.5.16.1.26
Novell Certification Conformance	Enable	1.3.6.1.4.1.18.3.5.5.16.1.15
GNS Response Mode	Alphabetical	1.3.6.1.4.1.18.3.5.5.16.1.29

IPX Interface Parameter Default Values

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. You can use the Configuration Manager to access and further modify or customize parameters belonging to a specific interface. This section describes all parameters shown on the IPX Interfaces window.

Table B-3. IPX Interface Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.17.1.2
Name	None	1.3.6.1.4.1.18.3.5.5.17.1.7
Cost	1 (for hop- or tick-based routing)	1.3.6.1.4.1.18.3.5.5.17.1.38
Host Number	None	1.3.6.1.4.1.18.3.5.5.17.1.25
Configured Encaps	Circuit medium dependent	1.3.6.1.4.1.18.3.5.5.17.1.40
TR End Station	Disable	1.3.6.1.4.1.18.3.5.5.17.1.59
NetBIOS Accept	Disable	1.3.6.1.4.1.18.3.5.5.17.1.60
NetBIOS Deliver	Disable	1.3.6.1.4.1.18.3.5.5.17.1.61
FR Broadcast (hex)	0xFFFFFF	1.3.6.1.4.1.18.3.5.5.17.1.28
FR Multicast (hex)	0xFFFFFF	1.3.6.1.4.1.18.3.5.5.17.1.30
Compress State	Disable	1.3.6.1.4.1.18.3.5.5.17.1.10
Compress Slot	16 (slots)	1.3.6.1.4.1.18.3.5.5.17.1.12
Checksum	Disable	1.3.6.1.4.1.18.3.5.5.17.1.39
SMDS Address (hex)	None	1.3.6.1.4.1.18.3.5.5.17.1.62
IPX Watchdog Spoofing	Disable	1.3.6.1.4.1.18.3.5.5.17.1.64
Delay	0	1.3.6.1.4.1.18.3.5.5.17.1.66
Stabilization Timer Delay	0	1.3.6.4.1.18.3.5.5.17.1.69
Throughput	0	1.3.6.1.4.1.18.3.5.5.17.1.67

IPX Change Circuit Parameter Default Values

This section describes how to set all parameters shown on the IPX Change Circuit window. The IPX circuit identifier appears in the window title.

Table B-4. IPX Change Circuit Parameter Default Values

Parameter	Default	MIB Object ID
Configured Network Number	None	1.3.6.1.4.1.18.3.5.5.17.1.22
Configured Encaps	Circuit Medium Dependent	1.3.6.1.4.1.18.3.5.5.17.1.40
Circuit Index	System-assigned	1.3.6.1.4.1.18.3.5.5.17.1.6
IPXWAN	Enable	Not Applicable
Common Network Number	None	1.3.6.1.4.1.18.3.5.5.17.1.24
Negotiated Protocols	Unnumbered RIP	1.3.6.1.4.1.18.3.5.5.17.1.8

IPX RIP Circuit Parameter Default Values

This section describes how to set all parameters shown on the IPX RIP Circuit window. The IPX circuit identifier appears in the window title.

Table B-5. IPX RIP Circuit Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.32.1.2
Mode	Standard	1.3.6.1.4.1.18.3.5.5.32.1.6
Pace	18 (packets/second)	1.3.6.1.4.1.18.3.5.5.32.1.7
Update Interval (sec)	60 (seconds)	1.3.6.1.4.1.18.3.5.5.32.1.8
Age Multiplier	6 (30-second increments, up to a total of 180 seconds)	1.3.6.1.4.1.18.3.5.5.32.1.9
Packet Size	432 (bytes)	1.3.6.1.4.1.18.3.5.5.32.1.10
Use Multicast	Yes	1.3.6.1.4.1.18.3.5.5.32.1.14
Split Horizon	Enable	1.3.6.1.4.1.18.3.5.5.32.1.15
Immediate Update	Enable	1.3.6.1.4.1.18.3.5.5.32.1.17

Table B-5. IPX RIP Circuit Parameter Default Values *(continued)*

Parameter	Default	MIB Object ID
Default Route Supply	Disable	1.3.6.1.4.1.18.3.5.5.32.1.18
Default Route Listen	Disable	1.3.6.1.4.1.18.3.5.5.32.1.19

IPX SAP Circuit Parameter Default Values

This section describes how to set all parameters shown on the IPX SAP Circuit window. The IPX circuit identifier appears in the window title.

Table B-6. IPX SAP Circuit Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.33.1.2
Mode	Standard	1.3.6.1.4.1.18.3.5.5.33.1.6
Pace	18 (packets/second)	1.3.6.1.4.1.18.3.5.5.33.1.7
Update Interval (sec)	60 (seconds)	1.3.6.1.4.1.18.3.5.5.33.1.8
Age Multiplier	6 (30-second increments, up to a total of 180 seconds)	1.3.6.1.4.1.18.3.5.5.33.1.9
Packet Size	480 (bytes)	1.3.6.1.4.1.18.3.5.5.33.1.10
Nearest Server Reply	Yes	1.3.6.1.4.1.18.3.5.5.33.1.11
NSQ Alphabetical	Yes	1.3.6.1.4.1.18.3.5.5.33.1.12
Use Multicast	Yes	1.3.6.1.4.1.18.3.5.5.33.1.16
Split Horizon	Enable	1.3.6.1.4.1.18.3.5.5.33.1.17
Immediate Update	Enable	1.3.6.1.4.1.18.3.5.5.33.1.19
Save Full Name	yes	1.3.6.1.4.1.18.3.5.5.33.1.20

IPX NetBIOS Static Route Configuration Parameter Default Values

This section describes all parameters shown on the IPX NetBIOS Static Route Configuration window.

Table B-7. NetBIOS Static Route Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Server	None	1.3.6.1.4.1.18.3.5.5.27.1.4
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.27.1.5

IPX NetBIOS Static Route Parameter Default Values

This section describes how to set all parameters shown on the IPX NetBIOS Static Routes window.

Table B-8. IPX NetBIOS Static Route Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.27.1.2
Target Server	None	1.3.6.1.4.1.18.3.5.5.27.1.5

Adjacent Host Configuration Parameter Default Values

This section describes all parameters shown on the Adjacent Host Configuration window.

Table B-9. Adjacent Host Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Host Number (hex)	None	1.3.6.1.4.1.18.3.5.5.26.1.5
WAN Address (hex)/ DLCI (decimal)	None	1.3.6.1.4.1.18.3.5.5.26.1.6

IPX Adjacent Hosts Parameter Default Values

This section lists all the parameters shown on the Adjacent Hosts window.

Table B-10. IPX Adjacent Hosts Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.26.1.2
WAN Address (hex)/ DLCI (decimal)	None	1.3.6.1.4.1.18.3.5.5.26.1.6

IPX Static Route Configuration Parameter Default Values

This section describes all parameters shown on the IPX Configuration window.

Table B-11. IPX Static Route Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.19.1.5
Next Hop Host (hex)	None	1.3.6.1.4.1.18.3.5.5.19.1.8

IPX Static Route Parameter Default Values

This section describes how to set all parameters shown on the IPX Static Routes window.

Table B-12. IPX Static Route Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.19.1.2
Hop Count	0	1.3.6.1.4.1.18.3.5.5.19.1.7
Ticks	0	1.3.6.1.4.1.18.3.5.5.19.1.6
Next Hop Host (hex)	None	1.3.6.1.4.1.18.3.5.5.19.1.8

IPX Static Service Configuration Parameter Default Values

This section describes all parameters shown on the IPX Static Services Configuration window.

Table B-13. IPX Static Service Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Service Name	None	1.3.6.1.4.1.18.3.5.5.23.1.5
Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.6
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.7
Host Number (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.8
Socket (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.9

IPX Static Services Parameter Default Values

This section describes how to set all parameters shown on the IPX Static Services window.

Table B-14. IPX Static Services Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.23.1.2
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.7
Host Number (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.8
Socket (hex)	None	1.3.6.1.4.1.18.3.5.5.23.1.9
Hop Count	None	1.3.6.1.4.1.18.3.5.5.23.1.10

Route Filter Configuration Parameter Default Values

This section describes all parameters shown on the IPX Route Filter Configuration window.

Table B-15. Route Filter Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.29.1.6
Target Network Mask	None	1.3.6.1.4.1.18.3.5.5.29.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.29.1.13

IPX Route Filter Parameter Default Values

This section describes how to set all the parameters shown on the IPX Route Filters window.

Table B-16. IPX Route Filter Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.29.1.2
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.29.1.6
Target Network Mask	None	1.3.6.1.4.1.18.3.5.5.29.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.29.1.13
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.29.1.8
Protocol	Any	1.3.6.1.4.1.18.3.5.5.29.1.10
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.29.1.9
Cost	None	1.3.6.1.4.1.18.3.5.5.29.1.11

SAP Network Filter Configuration Parameters

This section describes all parameters shown on the IPX Server Network Configuration window.

Table B-17. SAP Network Filter Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.6
Target Network Mask (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.7
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.8
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.30.1.14
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.30.1.9
Protocol	Any	1.3.6.1.4.1.18.3.5.5.30.1.11
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.30.1.10
Cost	None	1.3.6.1.4.1.18.3.5.5.30.1.12

IPX SAP Network-Level Filter Parameter Descriptions

This section describes all parameters shown on the IPX Service Network Filters window.

Table B-18. SAP Network-Level Filter Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.30.1.2
Target Network (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.6
Target Network Mask (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.7
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.30.1.8
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.30.1.14
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.30.1.9
Protocol	Any	1.3.6.1.4.1.18.3.5.5.30.1.11

Table B-18. SAP Network-Level Filter Parameter Default Values

Parameter	Default	MIB Object ID
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.30.1.10
Cost	None	1.3.6.1.4.1.18.3.5.5.30.1.12

IPX Server-Level Filter Configuration Parameter Descriptions

This section describes all parameters shown on the IPX Service Name Filter Configuration window.

Table B-19. IPX Server-Level Filter Configuration Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.31.1.2
Target Server	None	1.3.6.1.4.1.18.3.5.5.31.1.6
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.31.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.31.1.13
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.31.1.8
Protocol	Any	1.3.6.1.4.1.18.3.5.5.31.1.10
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.31.1.9
Cost	None	1.3.6.1.4.1.18.3.5.5.31.1.11

IPX SAP Server-Level Parameter Default Values

This section describes how to set all parameters shown on the IPX Server Name Filters window.

Table B-20. IPX SAP Server-Level Parameter Default Values

Parameter	Default	MIB Object ID
Enable	Enable	1.3.6.1.4.1.18.3.5.5.31.1.2
Target Server	None	1.3.6.1.4.1.18.3.5.5.31.1.6
Target Service Type (hex)	None	1.3.6.1.4.1.18.3.5.5.31.1.7
Filter Priority	None	1.3.6.1.4.1.18.3.5.5.31.1.13
Mode	Outbound	1.3.6.1.4.1.18.3.5.5.31.1.8
Protocol	Any	1.3.6.1.4.1.18.3.5.5.31.1.10
Action	Advertise/Accept	1.3.6.1.4.1.18.3.5.5.31.1.9
Cost	None	1.3.6.1.4.1.18.3.5.5.31.1.11

Appendix C
Common Service Types and Identifiers

Table C-1. Service Types and Identifiers

Service Type	Hexadecimal Identifier
Wildcard	FFFF
Unknown	0000
User	0001
User Group	0002
Print Queue	0003
NetWare File Server V3.*x*	0004
Job Server	0005
Gateway	0006
Print Server	0007
Archive Queue	0008
Archive Server	0009
Job Queue	000A
Administration	000B
Diagnostics	0017
NetBIOS	0020
NAS SNA Gateway	0021
NACS	0023

Table C-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Remote Bridge Server	0024
Bridge Server	0026
TCP/IP Gateway (Racal-Datacom)	0027
Eicon X.25 Point-to-Point GW	0028
Eicon 3270 Gateway	0029
(CHI) Corp	002A
Unknown	002C
Time Synchronization Server	002D
Archive Srvr Dynamic SAP/SMS TSA	002E
DI3270 Gateway	0045
Advertising Print Server	0047
TCP/IP Gateway (Racal-Datacom)	0048
Unknown	004A
Btrieve VAP 5.*x*	004B
NetWare SQL VAP/NLM	004C
Xtree Network Version	004D
Btrieve VAP 4.*x*	0050
QuickLink (Cubix)	0052
Print Queue User	0053
ARCserve VAP	0055
Eicon X.25 Multi-Point Gateway	0058
ARCserv	0064
ARCserve 3.0	0066
WANcopy Utility	0072
Cheyenne ARCserv 5.0 Intel	0077

Table C-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
TES-NetWare for VMS	007A
Emerald Backup/WATCOM Debugger	0092
TES-NetWare for VMS	0095
NetWare Access Server (NAS)	0098
SQL Server (Named Pipes)	009A
NetWare Access Server	009B
Portable NetWare/SunLink NVT	009E
Progress Database Server	009F
PowerChute APC UPS NLM	00A1
Compaq IDA Status Monitor	00AC
Unknown	0100
Intel LAN Protect Bindery	0102
Oracle Database Server	0103
NetWare 386, Remote Console	0107
Novell SNA Gateway	010F
HP Print Server	0112
CSA MUX	0114
CSA LCA	0115
CSA CM	0116
CSA SMA	0117
CSA DBA	0118
CSA NMA	0119
CSA SSA	011A
CSA STATUS	011B
CSA APPC	011E

Table C-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
SNA TEST (SAA profile)	0126
CSA TRACE	012A
Unknown	012E
Communications Executive	0130
NFS Domain Server	0133
NetWare Naming Service (NNS) Profile	0135
NNS Queue/NW Print Queue	0137
NNS Domain Scheme Descriptor	0138
Intel LANSpool VAP	0141
Aladdin Knowledge	0142
Optical Drives	0143
IrmaLAN Gateway	0152
Named Pipe Server	0154
Intel PICKIT/CAS Talk Server	0168
Unknown (User)	0173
Compaq SNMP Agent	0174
Xtree Server	0180
Xtree	0189
NetWare Access Server	018A
GARP Gateway (Net Research)	01B0
BindView (LAN Support Group)	01B1
Intel LanDesk Manager	01BF
Unknown	01CA
Shiva Netmodem	01CB
LanRover	01CC

Table C-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Castelle FAXPress Server	01D8
Castelle LANPress Print Server	01DA
Unknown	01E4
Legato	01F0
Legato	01F1
SQL Server	0200
NMA Agent (NMS; socket 0x2F90)	0233
LANZ Agent (Socket 0x401F; NetExp)	0237
LANZ Agent (Socket 0x4800)	0238
NMS Hub Management	0239
LANZ Agent (Socket 0x401F)	023A
NetWare SMS (Storage Management System)	023F
NetWare Connect	024E
NMS Console (name-stnMAC+IPX#)	026A
NW4 Time Sync Server (Socket 0x040)	026B
NW4 NDS Server	0278
NetWare for SAA Gateway	0304
Gallacticom BBS	030A
HP LaserJet (Quick Silver)	030C
Attachmate 3270 Gateway	0320
Multi Server Director	0327
Intel NetPort II	0361
ECS Cheyenne ARCserv 5.0 Intel	0375
Cheyenne ARC Serv 5.0 Intel SE	0376
PowerChute Version 3.0 (new)	037E

Table C-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
ViruSafe Notify	037F
HP Bridge	0386
HP Hub	0387
NetWare SAA Gateway	0394
Lotus Notes (OS/2 version)	039B
Central Point Anti Virus NLM	03B7
ARCserve 4.0 (socket 0x 8600)	03C4
Intel LANSpool 3.5	03C7
Lexmark 4033 Print Server	03D5
NetWare SQL/Gupta NLM	03DE
UNIXWare	03E1
UNIXWare	03E4
NetWare File Server Version 4.*x*	0400
NetSprint print server	0414
SiteLock Virus	0429
ARCserve 5.0	044C
Dell SCSI Array (SDA) Monitor	045B
SyBase	0474
SyBase	0475
Novix TCP/IP support NLM	04DC
SiteLock Checks	0520
Certus Anti Virus NLM (master)	0523
SiteLock Checks	0529
Delrina WinFax Pro network	0553
McAfee's NetShield anti-virus	0580

Table C-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
SiteLock	0B29
SiteLock Applications	0C29
SofTrack for NW Version 3.*x*	0C2C
LAI SiteLock	2380
Meeting Maker	238C
SofTrack for NW Version 4.*x*	2C0C
SiteLock Server (Brightworks)	4808
SiteLock User	5555
Tapeware	6312
Rabbit 3270 Gateway	6F00
Intel NetPort (Print Server)	8002
WordPerfect Network Version	8008
Unknown	8069
Unknown	8746
McAfee's NetShield anti-virus	9000
SQL Monitor (IPX)	9604
Unknown	9892
Unknown	C00C
SiteLock Metering VAP/NLM	F11F
SiteLock	F1FF
SQL Server (IPX)	F503

Appendix D
Sample IPX Configuration

This appendix provides a sample IPX configuration. Depending on the interface type and service requirements, the network uses different encapsulations. Configurations are provided for Router 1 and Router 2 (Figure D-1). The network configuration lists Router A and Router B but does not provide configurations for them.

The following assumptions apply:

- The router uses the tick-based RIP method
- The Frame Relay cloud is nonfully meshed and all PVCs are group mode. You have set the management type to default
- You have configured RIP for all interfaces
- You have enabled Multiple Host Addressing under IPX Global
- Default settings are in effect for all timer values

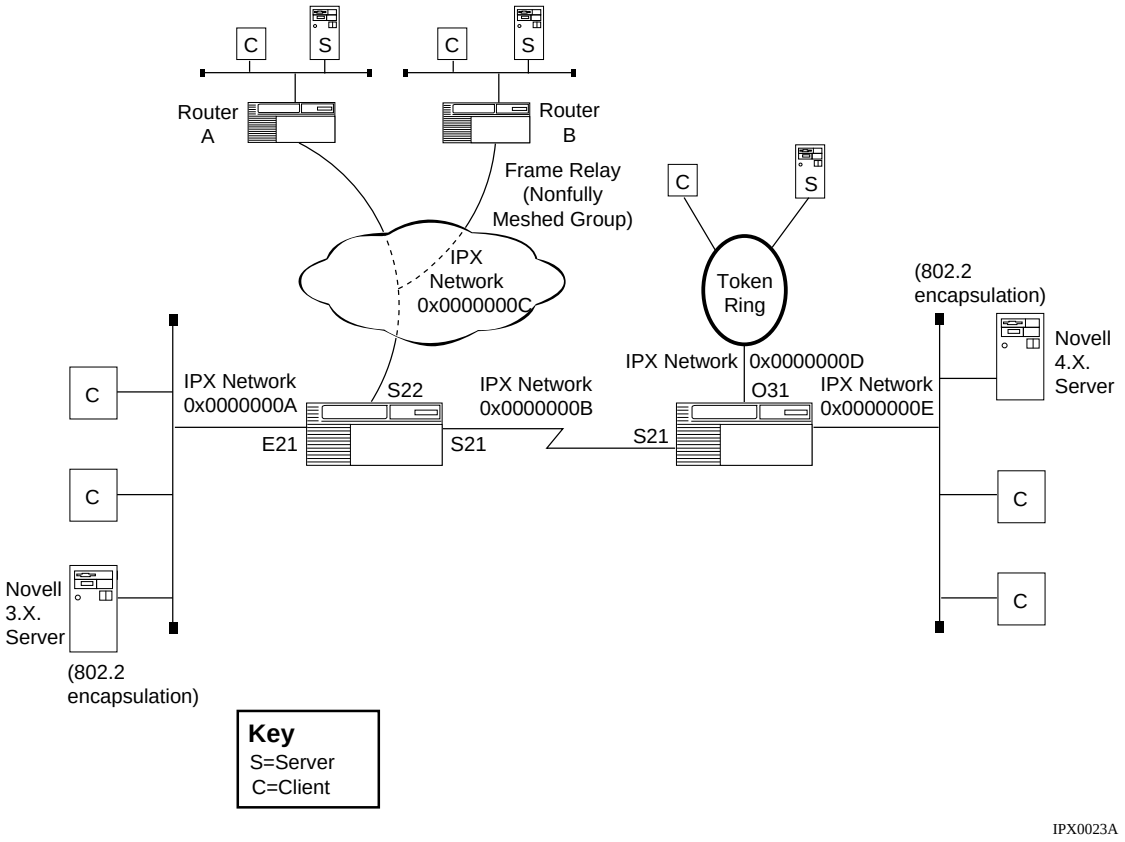

Figure D-1. Sample IPX Configuration

Configuration Particulars

Router 1

Edit the E21 circuit and add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000A and the Configured Encaps parameter to Novell.

Edit the S21 circuit and set the WAN protocol to Standard. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000B.

Edit the S22 circuit and set the WAN protocol to Frame Relay. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000C and click OK. Select Protocols > IPX > Interfaces, and highlight the IPX Network parameter, which should be set to 0x0000000C. Click on the RIP button and set the Split Horizon parameter to Disable.

Note: Turn off Split Horizon on the Frame Relay hub router if the spoke routers are to learn routes from each other. However, leave Split Horizon enabled on spoke routers.

Router 2

Edit the E21 circuit and add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000E.

Edit the S21 circuit and set the WAN protocol to Standard. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000B.

Edit the 031 circuit and set the ring speed to 16 MB. Add the IPX and RIP protocols. The IPX Configuration window appears. Set the Configured Network Number parameter to 0x0000000D and the Configured Encaps parameter to SNAP.

Index

A

accepting
  default configuration parameter values, 1-5
accessing IPX parameters
  using the Technician Interface, A-9
action
  SAP filters, 5-56
adding
  IPX route filters, A-64
  service network filter, A-71
adjacent host, 2-3
  configuration parameter descriptions, A-49
  parameter descriptions, A-51
advanced global parameters
  descriptions, A-21
  editing, A-21
advertisement interval (RIP), 5-18, 5-25
Age Multiplier
  IPX RIP circuit parameter, A-36
  IPX SAP circuit parameter, A-42
Aging Frequency
  advanced global parameter, A-18
Aging Pending Frequency
  advanced global parameter, A-18
ATM
  circuits, 5-14

B

bandwidth, 5-48, 5-50
bandwidth-on-demand, 5-42
Bay Networks
  CompuServe forum, xxvi
  Customer Service FTP, xxv
  home page on World Wide Web, xxv
  InfoFACTS service, xxvii
  publications, ordering, xxi
  support programs, xxiv
  Support Source CD, xxvi
  Technical Response Center, xxiii, xxvii
  technical support, xxiii
bindery
  and SAP, 5-24
bridge
  source route bridge endstation support, 5-67
broadcast filter
  NetBIOS, 5-37

C

change circuit parameters
  editing, A-39
characters in SAP pattern matching filters, 5-59
circuits
  LAN and WAN, 2-5
client/server connection
  example, 5-71
  role of Bay Networks router, 5-70
Common Network Number, 4-7
CompuServe, Bay Networks forum on, xxvi
concatenation rules and operators
  SAP pattern matching filters, 5-61
configurable RIP timers, 5-18
configurable SAP timers, 5-25
configurable split horizon, 5-20

configurations
IPX standard, 3-5
Configured Encaps
IPX interface parameter, A-25
configuring
RIP and SAP broadcast timers, 5-48
service network filter parameters, 5-63, A-71
configuring IPX
on a Token Ring interface, 3-8
connection negotiation
IPXCP, 4-9
IPXWAN, 4-10
connectionless datagram protocol, 2-2
Cost
IPX interface parameter, A-24
tick, 5-13
Customer Service FTP, xxv
customer support. *See* getting help

D

data link layer addresses, 3-6, 4-5
datagram, 2-2
default configuration parameter values
accepting or editing, 1-5
default route
support, 2-3
deleting
IPX from the router, 1-5
IPX route filters, A-71
service name filters, A-85
static routes, A-58
static services, A-64
deleting a service network filter, A-79
Destination Count
advanced global parameter, A-16
dial backup, 5-41
dial services
advantages of, 5-41
descriptions, 5-41
types of, 5-41
Dial-on-Demand, 2-3, 5-42
with static routing, 5-43, 5-50
with traffic filters, 5-44
dynamic routing, 2-3

E

editing
default configuration parameter values, 1-5
interface parameters, B-3
IPX change circuit parameters, A-39
IPX interface parameters, A-21
route filter configuration parameters, A-64
service name filter parameters, 5-64
static route parameters, A-56
static routes, A-53
static service parameters, A-61
editing IPX advanced global parameters, A-21
Enable
IPX interface parameter, A-22
encapsulation method, 3-3
encapsulation types. *See* frame encapsulation types
endstation support, 5-12, 5-67

F

filter
adding service network filters, A-71
deleting service name filters, A-85
editing service name filters, 5-64
NetBIOS broadcast, 5-37
SAP, 5-55
SAP filter concatenation rules and operators, 5-61
SAP filter pattern matching, 5-56
SAP filtering example, 5-63
SAP filters prohibiting SAP broadcasts, 5-31
SAP filters with pattern matching, 5-59
SAP pattern matching characters, 5-59
service name filter configuration parameters, A-79

service network filter parameters, 5-63, A-71, A-74
traffic filters with dial-on-demand, 5-44
filters
SAP filters with wildcards, 5-57
frame encapsulation types, 3-3, 3-9
frame formats, 2-5
Frame Relay, 4-2, 4-3
circuits, 5-14
fully meshed network, 5-20
split horizon enabled, 5-21

G

getting help
from a Bay Networks Technical Response Center, xxvii
from the Support Source CD, xxvi
through CompuServe, xxvi
through Customer Service FTP, xxv
through InfoFACTS service, xxvii
through World Wide Web, xxv
global parameters
advanced, descriptions, A-21
advanced, editing, A-21

H

HDLC encapsulation, 5-15
hop
as basis for routing decision, 5-12
definition, A-14
RIP maximum, 5-15
hop count, A-14
host
Router Host Number parameter, A-11
Host Count
advanced global parameter, A-17
host ID numbers
on a Token Ring circuit, 3-8
Host Number
adjacent host parameter, A-50
IPX interface parameter, A-24

I

Immediate Update
IPX SAP circuit parameter, A-45
InfoFACTS service, xxvii
information broadcast
RIP, 5-13
interface parameters
editing, A-21, B-3
Internet Data Packet (IDP) format, 2-2
internetwork addressing, 2-2
intranode addressing, 2-2
IPX
background information, 2-5
deleting IPX from the router, 1-5
IPX advanced global parameters
descriptions, A-21
editing, A-21
IPX change circuit parameters, A-39
IPX configurations
standard, 3-5
IPX interface parameters
editing, A-21
IPX over WAN media, 2-3
link configurations, 4-11
IPX parameters
accessing via Technician Interface, A-9
IPX ping, 5-12
IPX ping support, 5-69
IPX route filter parameters
descriptions, A-66
IPX service name filter
configuration parameter descriptions, A-79
parameter descriptions, A-81
IPX service network filter parameters
descriptions, A-74

IPX static service
configuration parameter descriptions, A-58
parameter descriptions, A-61
IPX watchdog acknowledgment, 5-44
IPX Watchdog Spoofing
IPX interface parameter, A-28
IPXCP, 2-3, 4-1
link configurations, 4-10
link negotiation, 4-9
sample configuration, 4-9
using, 4-2
IPXWAN, 2-3, 4-2
link configurations, 4-10
link negotiation, 4-10
sample configuration, 4-9
using, 4-2
IPXWAN connection
negotiating, 4-3

L

LAN
circuits, 2-5
logical, 3-3
physical, 3-3
link delay
WAN link, 4-3
link negotiation, 4-2
IPXCP, 4-9
IPXWAN, 4-10
load redistribution and rerouting, 5-6
load sharing, 5-4, 5-6, 5-12
Local IPX watchdog acknowledgment, 5-44
Log Filter
advanced global parameter, A-15
logical LAN, 3-3
logical network address, 3-3

M

MAC Address Override parameter, 3-9
MAC Address Select parameter, 3-9
Maximum Hops
advanced global parameter, A-16
Maximum Path
advanced global parameter, A-15
IPX advanced global parameter, 5-5
Maximum Path Splits
advanced global parameter, A-15
Multicast Address
IPX interface parameter, A-27
multiline, 2-5
multiline circuits, 5-7
differences from multipath, 5-8
multipath configurations, 5-7
multipath routing, 5-4, 5-12, A-15
precedence/priority, 5-6
multiple circuits per segment, 2-5
Multiple Host Address Enable parameter, 3-5
multiple interfaces per circuit, 2-5
multiple IPX interfaces per circuit, 2-3
multiple-host router, 2-5, 3-5

N

Name
IPX interface parameter, A-22
NCP
Network Control Protocol, 4-2
NDS (NetWare Directory Services, 5-24
Nearest Server Reply
IPX SAP circuit parameter, A-43
negotiation
IPXCP link, 4-9
IPXWAN connection, 4-3
IPXWAN link, 4-10
NetBIOS
broadcast packet (Type 20), 5-33
Type 20 broadcast packets, 5-12
NetBIOS Accept, 5-37

IPX interface parameter, A-26
NetBIOS broadcast filtering, 5-37
NetBIOS Deliver, 5-37
IPX interface parameter, A-26
NetBIOS packet
filtering, 5-39
use with nonstandard static routing, 5-36
use with standard static routing, 5-37
NetBIOS packet flow, 5-40
NetBIOS static routes
configuration parameter descriptions, A-45
parameter descriptions, A-47
NetWare
bindery, 5-24
Directory Services (NDS), 5-24
Novell, 3-4
network
fully meshed, 5-20
nonfully meshed, 5-21
network address
logical, 3-3
Network Control Protocol (NCP), 4-2
network number, 4-3
primary, 4-7
network numbers
setting for IPXCP, 4-4
setting for IPXWAN, 4-4
network-level services, 2-3
nonfully meshed network, 5-21
split horizon disabled, 5-22
Novell
NetWare, 3-4
standards, 5-49
Novell Certification Conformance
advanced global parameter, A-20
Novell, Inc., 2-2
number of IPX interfaces per circuit, 3-9

P

Pace
IPX RIP circuit parameter, A-36
IPX SAP circuit parameter, A-41
Packet Size
IPX RIP circuit parameter, A-37
IPX SAP circuit parameter, A-43
pattern matching
concatenation rules and operators, 5-61
SAP filters, 5-56, 5-59
periodic RIP advertisement interval, 5-18, 5-25
Permanent Virtual Circuit (PVC), 4-3
physical LAN, 3-3
ping, 5-69
ping capability, 5-12
PNN (primary network number), 4-7
PPP (point-to-point protocol), 4-2
precedence/priority
multipath routing, 5-6
Primary Net Number
IPX global parameter, A-21
primary network number (PNN), 4-7
purging
RIP entries, 5-18
PVC (Permanent Virtual Circuit), 4-3

R

regular expression (RE), 5-59
request packet (RIP), 5-13
response packet (RIP), 5-13
RFC
IPX source documents, 2-5
RFC 1552, 2-5, 4-1
RFC 1634, 2-5, 4-2
RIF (Routing Information Field), 5-67
RIP, 5-12, 5-13
RIP (Routing Information Protocol), 2-3

listen and supply functions, 5-17
maximum timer ticks, 5-15
update packet transmissions frequency, 5-48
RIP broadcast timers
configuring, 5-48
RIP information broadcast, 5-13
RIP request packet, 5-13
RIP response packet, 5-13
RIP timers
configurable, 5-18
route filter configuration parameters
editing, A-64
route filters
adding, A-64
deleting, A-71
dropping all routes, 5-54
parameter descriptions, A-66
router
deleting IPX from the router, 1-5
multiple-host, 2-5, 3-5
single-host, 2-5, 3-6
Router Host Number
IPX global parameter, A-11
Router Host Number parameter, 3-6
router information broadcast, 5-13
Router Name
IPX global parameter, A-7, A-11
router name
valid characters in, 4-8
routes
dropping all, 5-54
Routing Information Field (RIF), 5-67
Routing Information Protocol (RIP), 2-3, 5-12, 5-13
routing table, 5-13
running IPX over Frame Relay, 4-3
running IPX over PPP and Frame Relay, 4-2

S

SAP, 5-12
and NDS, 5-24
and the NetWare bindery, 5-24
SAP (Service Advertising Protocol), 2-3
SAP broadcast timers
configuring, 5-48
SAP filters, 5-61
example, 5-63
pattern matching, 5-56, 5-59
pattern matching characters, 5-59
prohibiting SAP broadcasts, 5-31
service network configuration parameters, A-71
wildcards and pattern matching, 5-57
SAP service
configuration parameters, A-58
deleting, A-64
SAP timer
configurable, 5-25
SAP update packet transmissions frequency, 5-48
Service Advertising Protocol (SAP), 2-3, 5-12
Service Count
advanced global parameter, A-17
service name filter parameters
editing, 5-64
service name filters
configuration parameter descriptions, A-79
deleting, A-85
parameter descriptions, A-81
service network filter
adding, A-71
configuration parameter descriptions, A-71
service network filter parameters
configuring, 5-63, A-71
descriptions, A-74
service network filters
dropping all services, 5-63
service types, C-1
services

dropping all, 5-63
Single Route Explorer (SRE) frame, 5-67
single-host router, 2-5, 3-6
Site Manager, 2-1
SMDS
circuits, 5-14
Socket
numbers, 2-2
source route bridge endstation support, 5-67
source routing, 5-12
split horizon, 5-12
configuring, 5-20
disabled in a nonfully meshed network, 5-22
enabled in a fully meshed network, 5-21
SRE frame, 5-67
standard IPX configurations
multiple-host router, 3-5
single-host router, 3-6
static routes
configuration parameter descriptions, A-53
deleting, A-58
NetBIOS configuration parameters, A-45
nonstandard NetBIOS use, 5-36
parameter descriptions, A-56
parameter editing, A-56
support, 2-3
using, A-53
with Dial-on-Demand, 5-43
with standard NetBIOS routing, 5-37
static service configuration parameters
descriptions, A-58
static service parameters
editing, A-61
static services
deleting, A-64
parameter descriptions, A-61
SAP service network configuration, 5-30
Support Source CD, xxvi

T

Target Network
IPX NetBIOS static route parameter, A-46, A-48
Target Server
IPX NetBIOS static route parameter, A-46
Technician Interface
accessing IPX parameters, A-9
tick
as basis for routing decision, 5-12
cost, 5-13
definition, 5-13, A-14
RIP timer maximum, 5-15
tick-based routing, 4-3
timeout
RIP entries, 5-18
timer
configurable SAP timers, 5-25
RIP (configurable), 5-18
RIP and SAP broadcast, 5-48
Token Ring
configuring host ID numbers, 3-8
Token Ring interface
configuring IPX on, 3-8
Token Ring line detail parameters
MAC Address Override, 3-9
MAC Address Select, 3-9
Token-Ring
endstation support, 5-67
TR End Station
IPX interface parameter, A-25
traffic filters
with Dial-on-Demand, 5-44
Type 20 broadcast packet
NetBIOS, 5-12, 5-33

U

Unnumbered RIP, 2-3
Update Interval

IPX RIP circuit parameter, 5-49, A-36
IPX SAP circuit parameter, 5-49, A-42
upper-layer protocol
handling packets associated with, 5-12

W

WAN
circuits, 2-5
link delay, 4-3
media, 4-2
watchdog acknowledgment, 5-44
watchdog spoofing parameter, A-28
wildcards
with SAP filters, 5-57
World Wide Web, Bay Networks home page on, xxv

X

Xerox Network System (XNS), 2-2